NDIA

Celebrating 20 Years of Systems Engineering Excellence

20th Annual Systems Engineering Conference

Conference Program

October 23-26, 2017 | Waterford at Springfield | Springfield, VA

NDIA.org/systemsengineering

Welcome to the NDIA Systems Engineering Conference

On behalf of the National Defense Industrial Association's Systems Engineering Division, I would like to extend a very warm welcome to the 20th Annual Systems Engineering Conference. Yes, the 20th Annual – who knew when we started this conference 2 decades ago that we would continue to have important systems engineering issues to address? Well, perhaps most of you - because after all, technology keeps moving, our military capability continues to increase, the complexity of our systems continues to grow, and the threats we have to address continue to grow at an alarming rate.

For example, 20 years ago the term "Cybersecurity" wasn't addressed in DoD circles. Interoperability wasn't considered. Systems-of-systems weren't mentioned. And today, these are some of our hottest issues that the entire defense-industrial complex seeks to successfully address, not to mention affordability, sustainability and a host of other issues that continue to need attention.

This conference is the primary one in the US that brings together the engineering arms of the Office of the Secretary of Defense, the Services, many of the Federal Agencies, and the defense industrial complex to address and seek solutions to the issues we all face. Executives, managers and engineers from all of the major US defense contractors, as well as the principal engineering executives, managers and engineers from the Department of Defense and the Services and Federal Agencies are here, and dialog among us is critical to achieving a mutual understanding of the issues we collectively face and desperately need to solve. This conference provides an outstanding opportunity to have that dialog and exchange ideas, so please take maximum advantage of this opportunity.

And if there is anything that the conference committee, whose names are listed in the program, or I, or the outstanding NDIA staff can do to assist you, please let us know.

Bob Rassa
Manager, Engineering Programs
Raytheon Space & Airborne Systems

Dear Attendees, Speakers and Sponsors,

I would like to add my warm welcome to those attending the annual Systems Engineering Division conference. This year's conference marks the 20th anniversary of this prestigious event. I congratulate the NDIA Systems Engineering Division for their sustained, superior performance in producing a highly consequential event and applaud the many ways the division supports the Defense Department and defense community.

This conference is the premier event addressing the application of systems engineering principles to defense acquisition. As such, it is the main forum to exchange information and ideas among the Defense Department, the services, defense agencies, industry and academia.

I wish the best of experiences here at the conference, and look forward to many more years of division engagement with the community to promote and refine the systems engineering practice.

Sincerely

Herbert J. Carlisle
General, USAF (Ret)
President and CEO

20TH ANNUAL SYSTEMS ENGINEERING CONFERENCE

OCTOBER 23-26, 2017 | SPRINGFIELD, VA

INTRODUCTION

Considered the major annual systems engineering event focusing on the performance of DoD programs and systems, the National Defense Industrial Association's Annual Systems Engineering Conference offers content tailored to all levels of systems engineering (SE) professionals:

- Keynote Presentation
- Systems Engineering Executive Panels
  - DoD Executive Panel: Service Systems Engineering Leads discuss SE issues
  - DoD Executive Panel: Interagency Systems Engineering Activity
  - Industry Executive Panel: Industry Leaders discuss Systems Engineering issues
  - DoD Executive Panel: Service and Agency Program Managers discuss systems engineering issues
- Technical Breakout Sessions (2+ days)

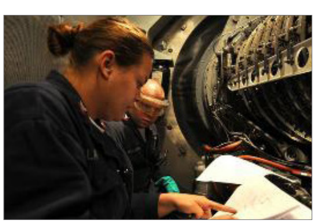
Demonstrating broad systems engineering community support, the conference is once again this year enjoying technical co-sponsorship by IEEE AES, IEEE Systems Council and the International Council on Systems Engineering.

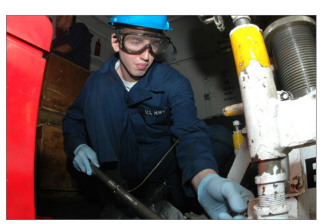
Further attesting to its value and relevance to Systems Engineering professionals within the defense industry, the conference continues to receive the support of the Office of the Deputy Assistant Secretary of Defense for Systems Engineering.

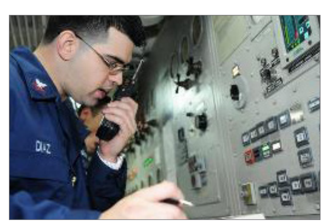
Major themes running through the three plus day agenda will include net-centric operations, data/information interoperability, system-of-systems engineering, cyber security and all aspects of system sustainment.

CONFERENCE OBJECTIVE

This conference seeks to create an interactive forum for Program Managers, Systems Engineers, Chief Scientists, Engineers, and Managers from the Requirements, Design, Verification, Support, Logistics and Test communities from both government and industry. The conference and the professional exchanges it will prompt will create opportunities to shape future policy and procedures.







BACKGROUND

The Department of Defense continues to seek ways to improve the acquisition of military equipment and capability to assist the warfighter in protecting the U.S. and its Allies around the world in a complex environment of ever-changing threats and conditions.

The Weapon Systems Acquisition Reform Act (WSARA) of 2009 defines Systems Engineering as a key enabler to effect improvements in defense acquisition and program execution that will produce more effective and affordable military systems. Previous DoD Better Buying Power initiatives, with their focus on achieving dominant capabilities through technical excellence and innovation, continued to emphasize the importance of engineering to the Department. The new administration seeks to increase military spending which will put additional onus on the defense industrial complex to achieve acquisition excellence, and systems engineering performance on the part of government and industry as partners is a key ingredient to success.

Systems Engineering is the “umbrella” engineering function that drives successful program execution and ensures an appropriate balance between requirements, performance, cost, schedule, and overall effectiveness and affordability. Systems Engineering principles embody strong technical and risk/opportunity management aspects for the acquiring Program Office as well as the prime and subcontractors. Strong emphasis on systems engineering throughout a program, especially in early development planning, is a key enabler of successfully fielding complex defense systems.

NDIA’s Annual Systems Engineering Conference explores the various roles of systems engineering from all aspects and perspectives—pragmatic, practical and academic—and brings key practitioners together to work on effective solutions to achieve a successful and affordable warfighting force.

CONFERENCE CHAIR

Mr. Robert Rassa
Director, Engineering Programs
Raytheon Company

DIVISION CHAIR

Mr. Frank Serna
Principal Director, Strategic Initiatives
Draper Laboratory

DIVISION VICE-CHAIR

Mr. Joseph Elm
Director of Engineering
L-3 Communications

NDIA PLANNING TEAM

Ms. Tammy Kicker, CMP
Director, Meetings & Events

Ms. Tina Fletcher
Meeting Planner, Meetings & Events

SCHEDULE AT A GLANCE

MONDAY, OCTOBER 23

8:00 am - 12:00 pm	Display Move In
12:00 pm - 5:30 pm	Registration
1:00 pm - 3:00 pm	Tutorials
3:00 pm - 3:30 pm	Networking Break
3:30 pm - 5:30 pm	Tutorials continue

TUESDAY, OCTOBER 24

7:00 am - 5:00 pm	Registration
7:00 am - 8:15 am	Networking Breakfast
8:15 am - 8:30 am	Opening Remarks: Bob Rassa, Raytheon; Frank Serna, Draper Labs
8:30 am - 9:30 am	Plenary Session Keynote: Vice Admiral Paul Grosklags, USN, Commander, Naval Air Systems Command
9:30 am - 10:00 am	Networking Break
10:00 am - 11:15 am	Executive Panel: DoD Systems Engineering
11:15 am - 12:30 pm	Executive Panel: Interagency Systems Engineering
12:30 pm -1:30 pm	Networking Luncheon
1:30 pm - 2:45 pm	Plenary Session Continues: Industry Executive Panel
2:45 pm - 3:00 pm	Presentation of Lt Gen Thomas R. Ferguson Systems Engineering Excellence Awards
3:00 pm - 3:30 pm	Networking Break
3:30 pm - 5:00 pm	Executive Panel: Program Managers
5:00 pm - 6:30 pm	Networking Reception

WEDNESDAY OCTOBER 25

7:00 am - 5:15 pm	Registration
7:00 am - 8:00 am	Networking Breakfast
8:00 am - 9:40 am	Concurrent Breakout Focus Sessions A
9:40 am - 10:15 am	Networking Break
10:15 am - 11:55 am	Concurrent Breakout Focus Sessions B
11:55 am - 1:00 pm	Networking Luncheon
1:00pm - 2:40 pm	Concurrent Breakout Focus Sessions C
2:40 pm- 3:15 pm	Networking Break
3:15 pm - 5:20 pm	Concurrent Breakout Focus Sessions D

THURSDAY OCTOBER 26

7:00 am - 5:15 pm	Registration
7:00 am - 8:00 am	Networking Breakfast
8:00 am - 9:40 am	Concurrent Breakout Focus Sessions A
9:40 am - 10:15 am	Networking Break
10:15 am - 11:55 am	Concurrent Breakout Focus Sessions B
11:55 am - 1:00 pm	Networking Luncheon
1:00 pm - 2:40 pm	Concurrent Breakout Focus Sessions C
2:40 pm- 3:15 pm	Networking Break
3:15 pm - 5:20 pm	Concurrent Breakout Focus Sessions D

TRACK OBJECTIVES

AGILE IN SYSTEMS ENGINEERING

Track Chairs: John Norton*, Raytheon Company*
Linda Maness*, Northrop Grumman Corporation*
Eileen Wrubel*, Software Engineering Institute*

Agile usage is becoming more prevalent within the government space. Lessons learned and ideas for implementation can be shared with those who are experienced in using Agile concepts. This track brings together practitioners with experience applying agile methods in a variety of disciplines and domains, with the goal of collaboration to expand their effective use in systems engineering and on defense programs

ARCHITECTURE

Track Chairs: Bob Scheuer*, The Boeing*
Ed Moshinsky, *Lockheed Martin Corporation*

Architecture is a key element in systems engineering. This track addresses architecture frameworks, strategies, and applications to improve system design, test, operations, and support.

COMPUTATIONAL RESEARCH & ENGINEERING ACQUISITION TOOLS AND ENVIRONMENTS (CREATE)

Track Chair: Douglass Post*, DoD High Performance Computing Modernization Program (HPCMP)*

The DoD HPCMP CREATE Program is a Tri-Service Program launched in 2006 by OSD and the HPCMP to develop and deploy eleven physics-based high performance computing software applications specifically to enable the DoD acquisition engineering community to design and analyze military ships, aircraft, ground vehicles, and radio frequency antennas. These tools enable engineers to generate an arbitrarily large number of design options (virtual prototypes expressed as digital product models) for design-space exploration, rapidly assess the feasibility and performance characteristics of each design option, and accurately predict the performance of each weapon platform with high-fidelity tools. With these tools, DoD engineers can identify design defects and performance shortfalls and fix them before metal has been cut, thus reducing costly rework and improving system performance. This reduces the cost, schedule, and risk of acquisition programs. The tools and computer time are available to DoD engineers (government and industry). The tools are being used by more than 180 DoD engineering organizations (government 40%, industry 50%, and other 10%--including academia) with over 1,400 users.

DEVELOPMENTAL TEST & EVALUATION (DT&E)

Track Chairs: Joe Manas*, Raytheon Company*

Developmental Test and Evaluation is a key aspect of successful systems engineering. This track addresses the entire continuum of test and evaluation from early planning to operational testing.

DIGITAL ENGINEERING/MODEL-BASED SYSTEMS ENGINEERING

Track Chair: Philomena Zimmerman, *DASD/SE*

Digital Engineering is an emerging set of practices for Systems Engineering and other engineering disciplines which has, at its core, the use of models (data, algorithms and/or processes) as a technical means of communication. When used properly, models can provide a cohesion across engineering activities, and cohesion with acquisition activities. When coupled with computational capabilities, resultant data from simulations can be used in decision-making at all echelons, and an increased level of insight and risk reduction in the end item can be achieved.

ENGINEERED RESILIENT SYSTEMS (ERS)

Track Chairs: Lois Hollan, *Potomac Institute*

Engineered Resilient Systems (ERS) is a Department of Defense priority initiative that seeks to transform engineering environments so that warfighting systems are more resilient and affordable across the acquisition lifecycle. The track will present new results across the ERS initiative including anchor technologies and computational representation.

EDUCATION & TRAINING

Track Chair: Don Gelosh*, Worcester Polytechnic Institute*

The Education and Training track for 2017 is an excellent collection of thirteen presentations from government, industry, and academia. The presentations describe a wide range of systems engineering workforce development activities from competency frameworks, cybersecurity skills, MBE and MBSE best practices, System of Systems guide and capstone marketplace to development of technical leaders.

ENTERPRISE HEALTH MANAGEMENT/PROGNOSTICS/ DIAGNOSTICS/RELIABILTY

Track Chairs: Chris Resig*, The Boeing Company*

The health of the system as a whole – the enterprise – is a critical function of systems engineering. This session will touch on some issues relating to the system health, including prognostics, diagnostics and reliability.

ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH (ESOH)

Track Chairs: Sherman Forbes*, USAF*
Dave Schulte*, SAIC*
Lucy Rodriguez*, Booz Allen Hamilton*

The ESOH track provides a cross section of topics that reflect the many different Systems Engineering design considerations included under the DoDI 5000.02 acronym ESOH, as defined in MIL-STD-882E, the DoD Standard Practice for System Safety. This year, Mr. James Thompson, Director, Major Program Support (MPS), within the Office of the Deputy Assistant Secretary of Defense for Systems Engineering will be the ESOH track's keynote speaker. Mr. Thompson will share his perspectives on Risk, Issue, and Opportunity (RIO) Management and Independent Technical Risk Assessments (ITRAs). Mr. David Asiello, the Acquisition, Sustainability & Technology Programs lead in the Office of the Assistant Secretary of Defense for Energy, Installations, and Environment will follow Mr. Thompson's presentation with a presentation focusing on how ESOH Risk Management is an integral part of the RIO Management Process and offering suggestions for improving the rigor, accountability, and visibility of ESOH risk management. There will be an extended question and answer period following Mr. Thompson's and Mr. Asiello's presentations to allow the audience to further explore the Acquisition and Sustainment Risk Management. The remainder of the ESOH track presentations will address specific acquisition ESOH issues, to include using Digital Engineering to manage ESOH risks and requirements, how to manage ESOH in Rapid Acquisitions, software system safety, hazardous materials regulations and management impacts on programs, environmental liabilities, environmental sustainability, and lessons learned about program office successes and failures in implementing the DoDI 5000.02 acquisition ESOH policy.

HUMAN SYSTEMS INTEGRATION (HSI)

Track Chair: Matthew Risser, *Pacific Science*
Patrick Fly, *The Boeing Company*

The HSI sessions include technical papers aligned with DoD HSI policy, standards and guidance. The goal is to address HSI implications in the design of complex systems in support of systems engineering and include HSI methods, metrics, and best practices, process improvements, applications and approaches to program integration.

INTEROPERABILITY/NET - CENTRIC OPERATIONS

Track Chairs: Jack Zavin, *OUSD/ATL*
John Daly, *Booz-Allen-Hamilton*

Interoperability is ability to operate in synergy in the execution of assigned tasks both within the DoD and its external mission partners. Net Centric Operations supports interoperability by providing the POPIM solution sets that allows the DoD and its mission partners to share information/data/knowledge when needed, where needed, and in a form they can understand and act on with confidence, while protecting it from those who should not have it. Net Centric Operations/Interoperability includes technologies such as Service Oriented Architecture, Data Center, Cloud Computing, information transport [e.g. internet, web, radios, data links], as well as both hardware and software [aka Information and Communicative Technology] together with people, operating alone or in organizations, as part of the System of Systems Systems Engineering.

MISSION ENGINEERING

Track Chair: Judith Dahmann, *MITRE*

Mission engineering (ME) is the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects. This track focuses on current directions in Defense ME and approaches to applying SoS and SE approach to ME.

MODELING AND SIMULATION (M&S)

Track Chairs: David Allsop, *The Boeing Company*
Chris Schreiber, *Lockheed Martin Corpration*

The M&S Track highlights the use of models and simulations in the systems engineering process. Included are presentations on integrated environments, tools & technologies, and M&S applications in several SE process phases. Topics focused specifically on Digital Engineering/Model-based Systems Engineering are contained in a separate track on this topic.

PROGRAM MANAGEMENT

Track Chairs: Ken Nidiffer, *Software Engineering Institute*

Program Managers and chief Systems Engineers should be the “joined-at-the-hip” leads on all programs that wish to be successful. This session will address some of the issues that our program managers face in the execution of programs.

SOFTWARE ENGINEERING

Track Chairs: Ken Nidiffer, *Software Engineering Institute*

Software is often overlooked when talking systems engineering yet software is a key element of most designs today and must always be part of the systems engineer’s portfolio of responsibility. This session will highlight a few significant software development issues.

SYSTEMS ENGINEERING EFFECTIVENESS

Track Chairs: Tim White, *Raytheon Company*
Joe Elm, *L3 Technologies*

Systems Engineering Effectiveness is obvious to some and quite esoteric to others. The goal though, improving the value obtained for each SE dollar spent, is shared by each who joins the discussion. Please attend the SE Effectiveness track to learn how your peers are implementing practical measures to better quantify the benefits of Systems Engineering and its value to Product Users and Developers alike. Early and effective Systems Engineering has been shown to return excellent value to all project stakeholders. This Track will highlight the latest DoD policy and guidance, define new approaches, and provide some practical experiences to assist the DoD and defense industry SE community in achieving a quantifiable and persistent improvement in program outcomes through appropriate application of systems engineering principles and best practices.

SYSTEMS OF SYSTEMS (SOS)

Track Chairs: Judith Dahmann, *MITRE*
Rick Poel, *The Boeing Company*
Jennie Horn, *Raytheon Company*

The System of Systems track will feature papers highlighting development SoS engineering approaches, particular SoS SE application areas, and SoS tools and modeling, including SoS SE applied to defense missions in mission engineering. See directly related track in Mission Engineering, above.

SYSTEM SECURITY ENGINEERING (SSE)

Track Chairs: Holly Dunlap, *Raytheon Company*
Melinda Reed, *DASD/SE*

System Security Engineering has become one of the most important aspects in the design of DoD systems. This track will focus on system security engineering and a holistic approach to program protection.

Monday, October 23

8:00AM - 12:00PM	**Display Move In**
12:00PM - 5:30PM	**Registration Open**
1:00 PM - 5:30 PM	**Tutorials**

Track	Room	Session	1:00PM - 1:30PM	1:30PM - 2:00PM	2:00PM - 2:30PM	2:30PM - 3:00PM
Track 4	Gibson	**Tutorial: Modeling and Simulation (M&S)** 1C4	19696 Half-Day Tutorial: Modeling and Simulation in the Systems Engineering Process ▶ Dr. Jim Coolahan, Coolahan Consultants, LLC			
Track 5	Sellier	**Tutorial: Applying MIL-STD** 1C5	19702 Tutorial: Tutorial: Applying Focused MIL-STD-882E Software Safety Level of Rigor ▶ Mr. Stuart Whitford, *Booz Allen Hamilton*			
Track 6	Korman	**Tutorial: Communication and Analysis** 1C6	19713 Effective Communication and Analysis in the Age of MBSE ▶ Mr. Ronald Kratzke, *Vitech Corporation*			

3:00PM - 3:30PM	**Networking Break**

Track	Room	Session	3:30PM - 4:00PM	4:00PM - 4:30PM	4:30PM - 5:00PM	5:00PM - 5:30PM
Track 4	Gibson	**Tutorial: Modeling and Simulation (M&S) Cont'd** 1D4	19696 Half-Day Tutorial: Modeling and Simulation in the Systems Engineering Process ▶ Dr. Jim Coolahan, Coolahan Consultants, LLC			
Track 5	Sellier	**Tutorial: Applying MIL-STD Cont'd** 1D5	19702 Tutorial: Applying Focused MIL-STD-882E Software Safety Level of Rigor ▶ Mr. Stuart Whitford, *Booz Allen Hamilton*			
Track 6	Korman	**Tutorial: Communication and Analysis Cont'd** 1D6	19713 Effective Communication and Analysis in the Age of MBSE ▶ Mr. Ronald Kratzke, *Vitech Corporation*			

5:30PM	**Adjourn**

Tuesday, October 24

7:00AM - 5:00PM	**Registration Open**
7:00AM - 8:15AM	**Networking Breakfast**

7:00AM - 5:00PM **Registration Open**

7:00AM - 8:15AM **Networking Breakfast**

8:15AM - 8:30AM **Opening Remarks**

Mr. Robert Rassa, *Director, Engineering Programs, Raytheon Company; NDIA Systems Engineering Conference Chair*

Mr. Frank Serna, *Principal Director, Strategic Initiatives, Draper Laboratory; Chair, NDIA Systems Engineering Division*

8:30AM - 9:30AM **Keynote Presentation**

VADM Paul Grosklags, *NAVAIR, Commander, Naval Air Systems Command*

9:30AM - 10:00AM **Networking Break**

10:00AM - 11:15AM **DoD Executive Panel: DoD Systems Engineering**

Moderator: Mrs Kristen Baldwin, *Deputy Assistant Secretary of Defense, Systems Engineering (Acting)*

Panelists:

- Col Laird Abbott, *USAF, Chief, Engineering and Force Management Division, Deputy Assistant Secretary for Science, Technology, and Engineering, SAF-AQR*
- Mr. William Bray, *USN, DASN RDT&E and Chief Systems Engineer*
- Mr. Douglas Wiltsie, *USA, Executive Director, SoSE&I, ASA ALT (invited)*

11:15AM - 12:30PM **Executive Panel: Interagency Systems Engineering**

Moderator: Ms. Kristen Baldwin, *Deputy Assistant Secretary of Defense, Systems Engineering (Acting)*

Panelists:

- Mr. Albert “Benjie” Spencer, *National Oceanic and Atmospheric Administration*
- Mr. Jon Holladay, *Technical Fellow for Systems Engineering, National Aeronautics and Space Admnistration*
- Mr. Kent Jones, Assistant Deputy Administrator for Systems Engineering and Integration, Defense Programs, DOE *National Nuclear Security Administration*
- Mr. Joseph Post, *Deputy Director, NAS Systems Engineering & Integration Federal Aviation Administration*
- Mr. James Tuttle, Deputy Director, CDS and Chief Systems Engineering, *Department of Homeland Security*

12:30PM - 1:30PM **Networking Luncheon**

1:30PM - 2:45PM **Industry Executive Panel: Model-Based Systems Engineering: How is it Helping?**

Mr. Frank Serna, *Principal Director, Strategic Initiatives, Draper Laboratory; Chair, NDIA Systems Engineering Division*

Panelists:

- Ms. Christi Gau Pagnanelli, *Director, BDS Systems Enginnering and Engineering Multi-Skilled Leadership, Boeing Defense, Space & Security*
- Mr. Randall Lum, *Corporate Director, Engineering, Northrop Grumman Corporation*
- Mr. Tim Walden, *Chief Engineer and Fellow, Lockheed Martin Corporate Engineering and Production Operations*
- Mr. Scott Welles, *Vice President, Booz Allen Hamilton*

2:45PM - 3:00PM **Presentation of Lt Gen Thomas R. Ferguson Systems Engineering Excellence Awards**

3:00PM - 3:30PM **Networking Break**

3:30PM - 5:00PM **Executive Panel: Program Managers**

Moderator: Col. David McIllece, USAF

Panelists:

- Col Edward Hospodar, USAF, *GPS User Equipment Senior Materiel Leader*
- COL Mike Milner, USA, *Armored Multi-Purpose Vehicle (AMPV) Program Manager*
- Col Amanda Myers, USAF, *Deputy Director, Global Reach Programs, Former C-17 System Program Manager*
- CAPT Seiko Okano, USN, *PEO Integrated Wardare Systems (IWS) 2.0 Program Manager*

5:00pm - 6:30pm **Networking Reception**

Wednesday, October 25

7:00AM-5:15PM **Registration**

7:00AM-8:00AM **Networking Breakfast**

Track	Chair	Session	8:00AM - 8:25AM	8:25AM - 8:50AM	8:50AM - 9:15AM	9:15AM - 9:40AM
Track 1	Singleton	**Human Systems Integration** 3A1	19516 Enhancing Future Soldier Systems through the use of the Systems Modeling Language to Incorporate Human Aspects into the Soldier as a System Definition ▶ Mr. Sean Pham, *U.S. Army ARDEC*	19641 HSI Best Practice Standard ▶ Dr. Patrick Fly, *The Boeing Company*	19739 The Human Systems Integration Partnership:: Delivering the HSI Capability to the Air Force Systems Engineering Process ▶ Mr. Derek Johnston, *United States Air Force*	19919 Adaptive Automation for UAV Pilot Vehicle Interfaces ▶ Mr. Jeff O'Hara, *Georgia Tech Research Institute*
Track 2	Miller	**Net Centric Operations & Interoperability** 3A2	19752 Kick Off/Context for NCO/I Track ▶ Mr. Jack Zavin, *DoD/OUSD(AT&L)*	19815 ISO/IEC/IEEE8 15288 System Interoperability Considerations ▶ Mr. John Daly, *Booz Allen Hamilton*	19759 JITC Executes DoD Mobility Field Assessments ▶ Mr. Khoa Hoang, *Joint Interoperability Test Command*	19764 Interface Management for Interoperability– from Theory to Modeling ▶ Mr. Matthew Hause, *PTC*
Track 3	Von Sternberg	**Engineering & Model-based Systems Engineering** 3A3	19819 DoD Digital Engineering Strategy ▶ Ms. Philomena Zimmerman, *Department of Defense*	19879 Model Centric Engineering Enabling a New Operational Paradigm for Acquisition ▶ Dr. Mark Blackburn, *Stevens Institute of Technology*	19853 Joint NDIA SSE & SwA Committee and Joint Federated Assurance Center, Government SwA Gap Analysis Workshop Summary ▶ Ms. Holly Dunlap, *Raytheon Company*	19855 MBSE and Systems Engineering Transformation ▶ Mr. Troy Peterson, *INCOSE*
Track 4	Gibson	**Modeling & Simulation** 3A4	19691 An Autonomous Sensor Tasking System ▶ Ms. Quintina Jones, *Raytheon Missile Systems*	19711 Best Practices for the Architecture, Design, and Modernization of Defense Models and Simulations ▶ Mr. Michael Heaphy, *AT&L/DMSCO*	19725 VV&A of Models and Simulations: The Power of Independent Cumulative Analyses ▶ Ms. Natalie Plotkin, *Raytheon Company*	19916 Formalized Execution of Model Integrated Descriptive Architecture Languages ▶ Mr. Gregory Haun, *Analytical Graphics, Inc.*
Track 5	Sellier	**Agile** 3A5	19877 Research Gone "Agile" A Case Study on Using an Enterprise Transformation Process to Enable Agile Methods in a Research Program ▶ Dr. Rosa Heckle, *The MITRE Corporation*	19726 Issues anOpportunities in Accelerated Software Development for Next Generation DoD Applications ▶ Dr. Craig Arndt, *Defense Acquisition University*	19755 A System Dynamics Model of the Scaled Agile Framework (SAFe) to Quantify the Effects of Management Decisions on Capability Development and Acquisition Outcomes ▶ Mr. Sean Ricks, *The MITRE Corporation*	19777 "Elicitation of Robust and Quality Agile User Stories Using QFD" ▶ Ms. Sabrina Ussery, *The George Washington University*
Track 6	Korman	**Software** 3A6	19745 Software Complexity Modeling ▶ Mr. Thuc Tran, *Capital One*	19749 Harnessing the Beast: Using Model Based Systems Engineering (MBSE) to Manage Complex Research Software Environments ▶ Ms. Jennifer Turgeon, *Sandia National Laboratories*	19758 Software Systems Maturity Analysis ▶ Mr. Christopher Dieckmann, *Idaho National Laboratory*	19816 Free and Open Source Tools to Assess Software Reliability and Security ▶ Mr. Lance Fiondella, *University of Massachusetts*

Wednesday, October 25 - Continued

9:40AM-10:15AM **Networking Break**

Track	Chair	Session	10:15AM - 10:40AM	10:40AM - 11:05AM	11:05AM - 11:30AM	11:30AM - 11:55AM
Track 1	Singleton	**Human Systems Integration** / **Systems Security Engineering** 3B1	19784 A Wearable Vision+Inertial Navigation System for Assessing Volumetric Utilization and Task Geometry Efficiency ▶ Mr. Kevin Duda, *Draper Laboratory*	19740 Fisher vs. Taguchi Experimental Design Methods in Human Factors ▶ Ms. Sarah Ewing, *Idaho National Laboratory*	19854 NDIA Welcome and Review of Accomplishments ▶ Ms. Holly Dunlap, *Raytheon Company*	19881 DoD Cyber Resilient Weapon Systems ▶ Ms. Melinda Reed, *Department of Defense*
Track 2	Miller	**Net Centric Operations & Interoperability** / **Mission Engineering** 3B2	19923 Joint and Mission Partner Interoperability ▶ Mr. Mike Richards, *Joint Staff J6*	19499 Real Life Cloud Acquisition and Adoption Across Agencies and Cloud Providers ▶ Mr. Mun-Wai Hon, *Noblis*	19849 Mission Integration Management, NDAA 2017 Section 855 ▶ Mr. Robert Gold, *Department of Defense*	19838 Systems of Systems Engineering Technical Approaches as Applied to Mission Engineering ▶ Dr. Judith Dahmann, *MITRE*
Track 3	Von Sternberg	**Digital Engineering & Model-based Systems Engineering** 3B3	19793 Model-Centric Decision Making: Insights from an Expert Interview Study ▶ Dr. Donna Rhodes, *Massachusetts Institute of Technology*	19890 Using MBSE to Communicate and Gain Acceptance of your Analysis ▶ Mr. Frank Salvatore, *Engility*	19795 New Innovations in Digital Systems Engineering ▶ Dr. Edward Kraft, *University of Tennessee Space Institute*	19920 Key MBSE Enablers with Examples ▶ Mr. Nicholas Driscoll, III, *Raytheon Company*
Track 4	Gibson	**CREATE Computational Research & Engineering Acquisition Tools and Environments** 3B4	20010 Digital Engineering (DE) and Computational Research and Engineering Acquisition Tools and Environments (CREATE) ▶ Ms. Philomena Zimmerman, *Department of Defense*	19721 CREATE: Accelerating Defense Innovation with Computational Prototypes and High Performance Computers ▶ Dr. Douglass Post, *DoD HPCMP*	19730 Physics-Based Simulation in Support of Acquisition program and Fleet Operations ▶ Mr. Steven Donaldson, *Naval Air Systems Command*	19728 Capstone: A Patform for Geometry, Meshing and Attribution Modeling for Physics-based Analysis and Design ▶ Dr. Saikat Dey, *US NRL Code 7131*
Track 5	Sellier	**Agile** / **Environment Safety & Occupational Health** 3B5	19902 Software Development Challenges in AFMC (Agile Software Development and Data Rights) ▶ Mr. Andrew Jeselson, *Air Force Materiel Command*		19701 Leveraging Cybersecurity Tools for Software Safety: Focusing (Some) Static Analysis on Safety-Critical Software ▶ Mr. Stuart Whitford, *Booz Allen Hamilton*	20028 Joint Software System Safety Implementation Guide ▶ Mr. Bob Smith, *Booz Allen Hamilton*
Track 6	Korman	**Systems Engineering Effectiveness** 3B6	19850 Engineering Autonomy ▶ Mr. Robert Gold, *Department of Defense*	19882 The Drive for Innovation in Systems Engineering ▶ Mr. Scott Lusero, *Department of Defense*	19814 DoD Systems Engineering Policy, Guidance and Standardization ▶ Ms. Aileen Sedmak, *Department of Defense*	19835 Helix: Understanding Systems Engineering Effectiveness through Modeling ▶ Ms. Nicole Hutchison, *Stevens Institute of Technology*

11:55AM - 1:00PM **Networking Luncheon**

Wednesday, October 25 - Continued

Track	Chair	Session	1:00PM - 1:25PM	1:25PM - 1:50PM	1:50PM - 2:15PM	2:15PM - 2:40PM
Track 1	Singleton	System Security Engineering 3C1	19852 NDIA Cyber Resilient & Secure Systems Summit Summary ▶ Ms. Holly Dunlap, *Raytheon Company*	19839 Unified Architecture Framework (UAF) Profile for Risk Assessment Methodology ▶ Ms. Tamara Hambrick, *Northrop Grumman Corporation*	19913 Considerations to Address Dependably Secure System Function in System Capability, Requirements, and Performance Artifacts ▶ Mr. Michael McEvilley, *The MITRE Corporation*	19866 AF Cyber Campaign Plan - Weapon Systems Focus ▶ Mr. Daniel Holtzman, *U.S. Air Force*
Track 2	Miller	Mission Engineering / System of Systems 3C2	19706 Model Based Systems of Systems Engineering ▶ Mr. Francis McCafferty, *Vitech Corporation*	19868 Mission Threads: Linking Mission Engineering and Systems Engineering ▶ Dr. Greg Butler, *Engility Corp*	19718 Developing Standards for Systems of Systems (SoS) Engineering ▶ Dr. Judith Dahmann, *The MITRE Corporation*	19804 Scaling Model-Based System Engineering Practices for System of Systems Applications: Software Tools ▶ Ms. Janna Kamenetsky, The *MITRE Corporation*
Track 3	Von Sternberg	Digital Engineering & Model-based Systems Engineering 3C3	19545 Pulling the Digital Thread with Model Based Engineering ▶ Mr. Christopher Finlay, *Raytheon Company*	19906 Modeling the Digital System Model Data Taxonomy ▶ Ms. Philomena Zimmerman, *Department of Defense*	19746 Developing and Distributing a CubeSat Model-Based Systems Engineering (MBSE) Reference Model – Interim Status #2 ▶ Dr. David Kaslow, *S.E.L.F*	19872 Enabling Design of Agile Security with MBSE ▶ Mr. Barry Papke, *No Magic*
Track 4	Gibson	CREATE: Computational Research & Engineering Acquisition Tools and Environments Engineering 3C4	19779 High-Fidelity Electromagnetic Modeling with CREATE-RF Tools ▶ Dr. Daniel Dault, *Air Force Research Lab*	19809 Physics Based Modeling & Simulation For Shock and Vulnerability Assessments - Navy Enhanced Sierra Mechanics ▶ Mr. Jonathan Stergiou, *Naval Surface Warfare Center, Carderock Division*	19823 The Role of CREATE-AV in Realization of the Digital Thread "Authoritative Truth Source" ▶ Dr. Edward Kraft, *University of Tennessee Space Institute*	19753 A Networked Frigate Concept Design Space Exploration Using the Rapid Ship Design Environment ▶ Dr. Douglas Rigterink, *Navel Surface Warfare Center, Carderock Division*
Track 5	Sellier	Environment Safety & Occupational Health 3C5	19912 DASD (SE) Risk, Issue, and Opportunity (RIO) Management and Independent Technical Risk Assessments (ITRAs) ▶ Mr. James Thompson, *Department of Defense*	19697 ESOH Risk Management ▶ Mr. David Asiello, *OASD(EI&E)*	19908 DoD Acquisition ESOH IPT Q&A Panel ▶ Mr. David Asiello, *OASD(EI&E)*	
Track 6	Korman	Systems Engineering Effectiveness 3C6	19790 Systems Engineering Research Needs and Workforce Development Study ▶ Dr. Dinesh Verma, *Systems Engineering Research Center (SERC)*	19744 Technical Performance Risk Management for Large Scale Programs ▶ Mr. Brian Davenport, *Raytheon Company*	19742 The Design of a Cone Penetrometer System ▶ Dr. Doris Turnage, *U. S. Army Engineer Research & Development Center*	19781 Additive Manufacturing – Challenges for the Systems Engineer and Program Manager ▶ Mr. William Decker, *Defense Acquisition University*

Wednesday, October 25 - Continued

2:40PM - 3:15PM **Networking Break**

			3:15PM - 3:40PM	3:40PM - 4:05PM	4:05PM - 4:30PM
Track 1	Singleton	**System Security Engineering** 3D1	19861 Cyber Resilient and Secure Weapon Systems Acquisition/Proposal Discussion & Summary ▶ Ms. Holly Dunlap, *Raytheon Company*	19771 When the Right Answer is Not What NAVSEA Normally Does ▶ Mr. Peter Chu, *NAVSEA 05*	19870 Can't We Just Get Along: Engineering Trade Decisions VS RMF at the System Level ▶ Mr. Don Davidson, *DoD CIO*
Track 2	Miller	**System of Systems** 3D2	19802 Scaling Model-Based System Engineering Practices for System of Systems Applications: Analytic Methods ▶ Dr. Aleksandra Markina-Khusid, The *MITRE Corporation*	19757 Defense System of Systems Gap Analysis ▶ Mr. Christopher Dieckmann, *Idaho National Laboratory*	19878 Enterprise Implications of Family of Systems (FoS) Acquisition ▶ Dr. Garrett Thurston, *Dassault Systemes*
Track 3	Von Sternberg	**Digital Engineering & Model-based Systems Engineering** 3D3	19775 Digital System Model Ice ▶ Dr. David Hench, *Eagle Ray R&D*	19871 Enabling Repeatable SE Cost Estimation with COSYSMO and MBSE ▶ Mr. Barry Papke, *No Magic*	19888 MBSE to Address Logical Text-Based Requirements Issues ▶ Dr. Saulius Pavalkis, *No Magic*
Track 4	Gibson	**CREATE: Computational Research & Engineering Acquisition Tools and Environments Engineering** 3D4	19693 Program Management in CREATE for the Development of Large-scale Physics-based Software Development Projects for Engineering Design and Analysis ▶ Dr. Richard Kendall, *DoD HPCMP*	19704 Computational Research and Engineering Acquisition Tools and Environments – Ground Vehicles (CREATE-GV) ▶ Dr. Christopher Goodin, *U.S. Army ERDC*	19715 Physics-based, Multidisciplinary Analysis of Fixed-Wing Aircraft with HPCMP CREATE(TM)-AV/Kestrel ▶ Dr. David McDaniel, *DoD HPCMP/CREATE*
Track 5	Sellier	**Environment Safety & Occupational Health** 3D5	19770 Assessing the impacts of Amended Toxic Substances Control Act to the DoD Mission and the Defense Industrial Base Panel ▶ Ms. Amy Borman, *U.S. Army* ▶ COL Joseph Constantino *(SAF/IEE)* ▶ Mr. Shane Esola, *DCMA* ▶ Mr. Jim Rudroff, (ODASN(E)) ▶ Dr. Patricia Underwood, *OASD(EI&E)*		
Track 6	Korman	**Systems Engineering Effectiveness** 3D6	19738 Improving Effectiveness with respect to Time-To-Market and the Impacts of Late-stage Design Changes in Rapid Development Life Cycles ▶ Mr. Parth Shah, *George Washington University*	19716 Integrity System Security Engineering into System Engineering ▶ Mr. Ken Barker, *USAF*	19824 Implementation of the R&M Engineering Body of Knowledge ▶ Mr. Andrew Monje, *Department of Defense*

Wednesday, October 25 - Continued

			4:30PM - 4:55PM	4:55PM - 5:20PM	
Track 1	Singleton	**System Security Engineering** 3D1	19880 Engaging the DoD Enterprise to Protect U.S. Military Technical Advantage: Joint Acquisition Protection and Exploitation Cell Update ▶ Mr. Brian Hughes, *Department of Defense*	19798 Using Real Options Analysis to develop Resiliency in System Security Architectures ▶ Mr. Chris D'Ascenzo, *Defense Acquisition University*	
Track 2	Miller	**System of Systems** 3D2	19736 "Defense Acquisition System" System of Systems Engineering ▶ Mr. Larry Harding, *Idaho National Laboratory*		
Track 3	Von Sternberg	**Digital Engineering & Model-based Systems Engoneering** 3D3	19763 The Digital Engineering Journey ▶ Mr. Mathew Hause, *PTC*	19833 Digitalization of Systems Engineering –Examples and Benefits for the Enterprise ▶ Mr. Sanjay Khurana, *Dassault Systemes*	
Track 4	Gibson	**CREATE: Computational Research & Engineering Acquisition Tools and Environments Engineering** 3D4	19776 Weapons System Innovation through Workflow-based Computational Prototyping ▶ Mr. Loren Miller, *DataMetric Innovations, LLC*	19786 Rotorcraft Acquisition: Development of Modeling and Simulation Procedures ▶ Dr. Marvin Moulton, *U.S. Army*	
Track 5	Sellier	**Environment Safety & Occupational Health** 3D5	19770 Assessing the impacts of Amended Toxic Substances Control Act to the DoD Mission and the Defense Industrial Base Panel ▶ Ms. Amy Borman, *U.S. Army* ▶COL Joseph Constantino *(SAF/IEE)* ▶ Mr. Shane Esola, *DCMA* ▶ Mr. Jim Rudroff, (ODASN(E)) ▶ Dr. Patricia Underwood, *OASD(EI&E)*		
Track 6	Korman	**Systems Engineering Effectiveness** 3D6	19762 Decision-Driven Product Development ▶ Mr. Matthew Hause, *PTC*	19830 Are We Doing Enough in Requirements Management? ▶ Dr. Steven Dam, *SPEC Innovations*	

5:20PM **Adjourn**

Thursday, October 26

7:00AM-5:15PM **Registration**

7:00AM-8:00AM **Networking Breakfast**

			8:00AM - 8:25AM	8:25AM - 8:50AM	8:50AM - 9:15AM	9:15AM - 9:40AM
Track 1	Singleton	**System Security Engineering** 4A1	19796 Cyber Systems Risk – an Opportunity for Model Based Engineering & Design ▶ Dr. Jerry Couretas, *Booz Allen Hamilton*	19785 Cybersecurity As An Integral Part of Systems Engineering ▶ Mr. William Decker, *Defense Acquisition University*	19741 Security at Design Time: Addressing Resilience in Mission Critical Cyber-Physical Systems ▶ Mr. Thomas McDermott, Jr., *Georgia Tech Research Institute*	19911 Achieving DoD Software Assurance (SwA) ▶ Mr. Thomas Hurt, *Department of Defense*
Track 2	Miller	**Developmental Test & Evaluation** 4A2	19792 An Approach to Verification of Complex Systems ▶ Dr. Wilson Felder, *Stevens Institute of Technology*	19925 Improving Distributed Testing with TENA and JMETC ▶ Mr. Ryan Norman, *TENA / JMETC*	19774 Identifying Requirements and Vulnerabilities for Cybersecurity; Or How I Learned to Stop Worrying and Love the Six-Phase Cybersecurity T&E Process ▶ Mr. David Brown, *Electronic Warfare Associates (EWA)*	19831 How Can We Use V&V Techniques in Early Systems Engineering? ▶ Dr. Steven Dam, *SPEC Innovations*
Track 3	Von Sternberg	**Engineered Resilient Systems** 4A3	20009 Digital Engineering and ERS ▶ Mr. Robert Gold, *Department of Defense*		19845 ERS: Influencing Acquisition Innovation ▶ Dr. Owen Eslinger, *U.S. Army Engineer Research and Development Center*	19907 Scaling Data Analytics for ERS ▶ Mr. David Stuart, *U.S. Army Engineer Research and Development Center*
Track 4	Gibson	**Create: Computational Research & Engineering Acquisition Tools and Environments Engineering** 4A4	19887 Multi-Disciplinary Integration of ModSim for Navy Applications ▶ Dr. Greg Bunting, *Sandia National Laboratories*	19729 Academic Deployment of the HPCMP CREATE Genesis Software Package ▶ Dr. Robert Meakin, *U.S. DoD HPCMP*	19875 Secure Web-Based Access for Productive Supercomputing ▶ Ms. Laura Ulibarri, *Air Force Research Laboratory*	19800 CREATE-SH IHDE: Workflow Process Improvements for Hydrodynamics Characterization of Ship Designs ▶ Mr. Wesley Wilson, *Naval Surface Warfare Center, Carderock Division*
Track 5	Sellier	**Environment, Safety & Occupational Health** 4A5	19773 Model Based Systems Engineering (MBSE) Considerations for Environment Safety and Occupational Health (ESOH) ▶ Mr. Leo Kilfoy, *MSC Software*	19772 A Pragmatic Approach to System Modeling for Hazard Identification and Risk Management ▶ Mr. Michael Vinarcik, *Booz Allen Hamilton*	19708 Unmanned System (UxS) Safety Engineering Precepts - an OSD Guide - update of the 2007 OSD UxS Safety Guide ▶ Mr. Michael Demmick, *NOSSA*	19754 Divergent Oscillating Refueling Probe on the HH-60G Pavehawk ▶ Mr. Joseph Jones, *SAF/AQRE*
Track 6	Korman	**Architecture** 4A6	19820 MOSA Considerations in Systems Engineering Through the Lifecycle ▶ Ms. Philomena Zimmerman, *Department of Defense*	19821 Implementing a MOSA to Achieve Acquisition Agility in Defense Acquisition Programs ▶Ms. Philomena Zimmerman, *Department of Defense*	19837 Challenges to Implementing MOSA for Major DoD Acqusition Programs ▶ Mr. Edward Moshinsky, *Lockheed Martin Corporation*	19778 Investigating Approaches to Achieve Modularity Benefits in the Defense Acquisition Ecosystems ▶ Dr. Navindran Davendralingam, *Purdue University*

THURSDAY, OCTOBER 26- CONTINUED

9:40AM-10:15AM **Networking Break**

Track	Chair	Session	10:15AM - 10:40AM	10:40AM - 11:05AM	11:05AM - 11:30AM	11:30AM - 11:55AM
TRACK 1	SINGLETON	**System Security Engineering** 4B1	19853 Joint NDIA SSE & SwA Committee and Joint Federated Assurance Center, Government SwA Gap Analysis Workshop Summary ▶ Ms. Holly Dunlap, *Raytheon Company*	19698 Program Manager's Guidebook for Integrating Software Assurance into Defense Systems During the System Acquisition Lifecycle ▶ Dr. Kenneth Nidiffer, *Software Engineering Institute*	19735 Reducing Software Vulnerabilities – The "Vital Few" Process and Product Metrics ▶ Mr. Girish Seshagiri, *Ishpi Information Technologies, Inc.*	19910 DoD Joint Federated Assurance Center (JFAC) 2017 Update ▶ Mr. Thomas Hurt, *Department of Defense*
TRACK 2	MILLER	**Education & Training** 4B2	19813 Shaping the Department of Defense Engineering Workforce ▶ Ms. Aileen Sedmak, *Department of Defense*	19794 Review of Best Practices for Technical Leadership Development ▶ Dr. Wilson Felder, *Stevens Institute of Technology*	19805 Development of a Defense Mission Engineering Competency Model ▶ Dr. Nicole Hutchison, *Stevens Institute of Technology*	19789 The Capstone Marketplace: Growing our Technical Workforce through Systems Oriented Senior Design Projects ▶ Ms. Megan Clifford, *Systems Engineering Research Center*
TRACK 3	VON STERNBERG	**Engineered Resilient Systems** 4B3	19844 Tradespace: Informed Decision making for Acquisition ▶ Mr. Timothy Garton, *Engineer Research and Development Center*	19834 Building an Agile Framework for the Analysis of Environmental Impacts on Military Systems ▶ Dr. Dharhas Pothina, *Engineer Research and Development Center*	19859 Introducing Lifecycle Cost to Early Conceptual Tradespace Exploration ▶ Mr. Erwin Baylot, *Engineer Research and Development Center*	19806 Overcoming the Government - Industry Collaboration Hurdle ▶ Dr. Patrick Martin, *BAE Systems*
TRACK 4	GIBSON	**Create: Computational Research & Engineering Acquisition Tools and Environments Engineering** 4B3	19694 Software Engineering for Physics-based HPC Applications for Engineering Design and Analysis in CREATE ▶ Dr. Richard Kendall, *DoD HPCMP*	19703 Verification and Validation in CREATE Multi-Physics HPC Software Applications ▶ Dr. Lawrence Votta, *Brincos Inc.*	19709 DoD Risk Management Deficiencies...And How to Fix Them ▶ Mr. Richard Sugarman, *U.S. Air Force*	19724 Tools for Acquiring Highly Maintainable Software-Intensive Systems ▶ Dr. Barry Boehm, *USC*
TRACK 5	SELLIER	**Environment, Safety & Occupational Health** 4B5	19767 Rapid Equipping – Immediate Need to Equip and Protect Soldiers ▶ Mr. George Evans, *Prospective Technology Inc. (SAAL-PE/PTI ctr)*	19769 ESOH Risk Management and Applying MIL-STD-882E Principles to Programs that Deviate from Standard Acquisition Models ▶ Mr. Jefferson Walker, *Booz Allen Hamilton*	19732 Hazardous Materials Risk Management Using MIL-STD-882E ▶ Ms. Lori Hales, *Booz Allen Hamilton*	19836 Leveraging the International Aerospace Environmental Group (IAEG) Defense Acquisition Materials Declaration Process ▶ Ms. Karen Gill, *Booz Allen Hamilton*
TRACK 6	KORMAN	**Architecture** 4B6	19780 Cybersecurity and a Modular Open Systems Approach ▶ Mr. William Decker, *Defense Acquisition University*	19743 If System Architectures are So Useful, Why Don't We Use Them More? ▶ Mr. Robert Scheurer, *NDIA SE Architecture Committee*	19873 A Reverse Chronology of Evolutionary Architecture and Agile Development ▶ Mr. Thomas Mielke, *CACI International Inc.*	19903 Efficient Use of Enterprise and System Architecting in Combined Environment ▶ Dr. Howard Gans, *Harris Corporation*

Thursday, October 26 - Continued

11:55AM - 1:00PM **Networking Luncheon**

			1:00PM - 1:25PM	1:25PM - 1:50PM	1:50PM - 2:15PM	2:15PM - 2:40PM
Track 1	Singleton	**System Security Engineering** 4C1	19862 Long-Term Strategy for DoD Trusted and Assured Microelectronics Needs ▶ Dr. Jeremy Muldavin, *Department of Defense*	19747 SSE Abstract: Developing Trust For a Secure Microelectronics Supply Chain ▶ Dr. Michael Fritze, *Potomac Institute for Policy Studies*	19731 SSE: Trusted Microelectronics Joint Working Group ▶ Dr. Brian Cohen, *Institute for Defense Analyses*	19700 Managing Risk with Trusted ASICs: Introducing to the SSE Community a Guidebook to Using Trusted Suppliers ▶ Mr. Jim Gobes, *Intrinsix Corp.*
Track 2	Miller	**Education & Training** 4C2	19811 Version 1.0 of the New INCOSE Competency Framework ▶ Mr. Don Gelosh	19515 A Proposed Engineering Training Framework and Competency Methodology ▶ Dr. Eric Dano, *BAE Systems*	19695 Educating Engineers or Training Technicians ▶ Mr. Zane Scott, *Vitech Corporation*	19734 Solving Cybersecurity Skills Shortage With Apprenticeships & Certifications – A Case Study ▶ Mr. Girish Seshagiri, *Ishpi Information Technologies, Inc.*
Track 3	Von Sternberg	**Engineered Resilient Systems** 4C3	19783 The Language of Complexity: Ontology in Systems Design and Engineering ▶ Mr. Abe Wu, *Raytheon Missiles*	19846 Physics and Model Based Aerodynamic Design and Analysis at GA ▶ Mr. Pritesh Mody, *General Atomics Aeronautical Systems, Inc.*	20050 Automation and Integration for Complex System Design ▶ Mr. Scott Radon, *Phoenix Integration*	19825 Application of CREATE Tools for High Fidelity Design Space Exploration ▶ Mr. Antonio De La Garza, *Lockheed Martin Aeronautics Company*
Track 4	Gibson	**Program Management** 4C4	19751 A Capability Value Frontier in Support of Acquisition Approaches to Enable Military Effectiveness ▶ Dr. Marilyn Gaska, *Lockheed Martin Corporation*	19782 Technical Data Package and Intellectual Property Rights ▶ Mr. William Decker, *Defense Acquisition University*		19827 Policy Engineering: Applying Systems Engineering to Develop Better Policies ▶ Dr. Steven Dam, *SPEC Innovations*
Track 5	Sellier	**Environment, Safety & Occupational Health** 4C5	19714 DoD's REACH Strategy and its Impact to Acquisition and Sustainment ▶ Dr. Patricia Underwood, *OASD(EI&E)*	19705 Environmental Liabilities for DoD Weapons Systems ▶ Ms. Patricia Huheey, *OASD(EI&E)*	19810 *Environmental Life Cycle Assessment of Commercial Transportation Activities* ▶ Ms. Sheila Neumann, *University of Texas at Arlington*	19699 LIfe Cycle Assessment: A Tool for Protecting Defense Assets ▶ Dr. Kelly Scanlon, *OASD(EI&E)*
Track 6	Korman	**Architecture** 4C6	19748 Advancing U.S. Marine Corps Warehouse Management Operations Through System Architecture and Analysis ▶ Mr. Christopher Melkonian, *Marine Corps Systems Command*	19828 From Architecture to Operations – Using Your Architecture Work in Operations ▶ Dr. Steven Dam, *SPEC Innovations*		

Thursday, October 26 - Continued

2:40PM - 3:15PM **Networking Break**

Track	Chair	Session	3:15PM - 3:40PM	3:40PM - 4:05PM	4:05PM - 4:30PM
Track 1	Singleton	**System Security Engineering** 4D1	19864 Field Programmable Gate Array (FPGA) Assurance ▶ Mr. Ray Shanahan, *Department of Defense*	19891 Using Cyber Resiliency Frameworks to Engineer and Manage IT Services ▶ Dr. Subash Kafle, *The MITRE Corporation*	19863 Survey of Cyber Security Framework across Industries ▶ Mr. Ambrose Kam, *Lockheed Martin Corporation*
Track 2	Miller	**Education & Training** 4D2	19756 Teaching Executable Model-Based Engineering (MBE): Best Practices ▶ Mr. Matthew Cotter, *The MITRE Corporation*	19760 The Systems of Systems (SoS) Primer: A Guide to SoS for all Expertise Levels ▶ Ms. Laura Antul, *The MITRE Corporation*	19865 Breaking Out: Systems Engineering To Go ▶ Mr. Zane Scott, *Vitech Corporation*
Track 3	Von Sternberg	**Engineered Resilient Systems** 4D3	19712 Implementation of Clustering Analysis in Engineered Resilient Systems Tools for Enhanced Trade Space Exploration of Military Ground Vehicles ▶ Mr. Andrew Pokoyoway, *TARDEC*	19818 Tradespace Analysis and Exploration incorporating Reliability, Availability, Maintainability, and Cost ▶ Dr. Lance Fiondella, *University of Massachusetts*	19741 Security at Design Time: Addressing Resilience in Mission Critical Cyber-Physical Systems ▶ Mr. Thomas McDermott, *Georgia Tech Research Institute*
Track 4	Gibson	**Program Management** 4D4	19847 Proactively Managing Supplier Relationships for an Integrated Product Development Program ▶ Ms. Beth Layman, *Layman & Layman*	19932 Improving Efficiency in Assembly, Integration and Test (AI&T) ▶ Mr. Jeff Juranek, *The Aerospace Corporation*	19842 "Other Transactions" - An Alternative to Business as Usual ▶ Mr. Richard Dunn, *Strategic Inst for Innovation in Govt Contracting*
Track 5	Sellier	**Environment, Safety & Occupational Health** 4D5	19766 ESOH Management in Agile and Rapid Acquisitions Using Digital Engineering ▶ Mr. Sherman Forbes, *SAF/AQRE*		
Track 6	Korman	**Enterprise Health Management** 4D6	19523 Mission-Based Forecasting for the Sustainment Enterprise ▶ Col Greg Parlier, USA (Ret.), *GH Parlier Consulting*		

Thursday, October 26 - Continued

			4:30PM - 4:55PM	4:55PM - 5:20PM	
Track 1	Singleton	System Security Engineering 4D1	19722 The Systems Challenges of Cybersecurity ▶ Mr. Jeffery Zili, *Vitech*	19895 Modeling Cyber Security ▶ Mr. Ambrose Kam, *Lockheed Martin Corporation*	
Track 2	Miller	Education & Training 4D2	19914 Bridging the Gap to MBSE ▶ Mr. James Baker, *Sparx Systems*	19719 Introducing Cyber Resiliency Concerns Into Engineering Education ▶ Mr. Thomas McDermott, *Georgia Tech Research Institute*	
Track 3	Von Sternberg	Engineered Resilient Systems 4D3	19781 Additive Manufacturing – Challenges... Program Manager ▶ Mr. William Decker, *DAU Huntsville*	20051 Model-Based Engineering: Opportunities, Risks, and Best Practices ▶ Dr. Marc Halpern, *Gartner, Inc.*	

5:20PM **Adjourn Conference**

SILVER SPONSORS

At IBM Research, we invent things that change the world. We are pioneering promising and disruptive technologies that will transform industries and society, including the future of AI, blockchain and quantum computing.

We are driven to discover. We are home to more than 3,000 researchers in 12 labs located across six continents. Scientists from IBM Research have produced six Nobel Laureates, 10 U.S. National Medals of Technology, five U.S. National Medals of Science, 6 Turing Awards, 19 inductees in the National Academy of Sciences and 20 inductees into the U.S. National Inventors Hall of Fame.

Our teams are pushing the boundaries of science to uncover tomorrow's breakthroughs for national security, economic growth and jobs. We are especially focused on microelectronics as a national critical resource. The semiconductor industry is a foundational industry for modern society. Semiconductors enable all electronics; they are at the base of the electronics food chain and make digital life – every electronics system in the world – possible. Technological leadership in semiconductor research, development, design and manufacturing is vital for economic growth and especially for national security.

"Headquartered in Bethesda, Maryland, Lockheed Martin is a global security and aerospace company that employs approximately 97,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services."

Raytheon Company is a technology and innovation leader specializing in defense, security and civil markets throughout the world. With a history of innovation spanning more than 90 years, Raytheon provides state-of-the-art electronics, mission systems integration and other capabilities in the areas of sensing; effects; and command, control, communications and intelligence systems; as well as a broad range of mission support services.

THANK YOU TO OUR SPONSORS

Outpacing the Competition: A Systems Engineering Challenge

24 October 2017

Presented To:

NDIA Systems Engineering Conference

Presented By:

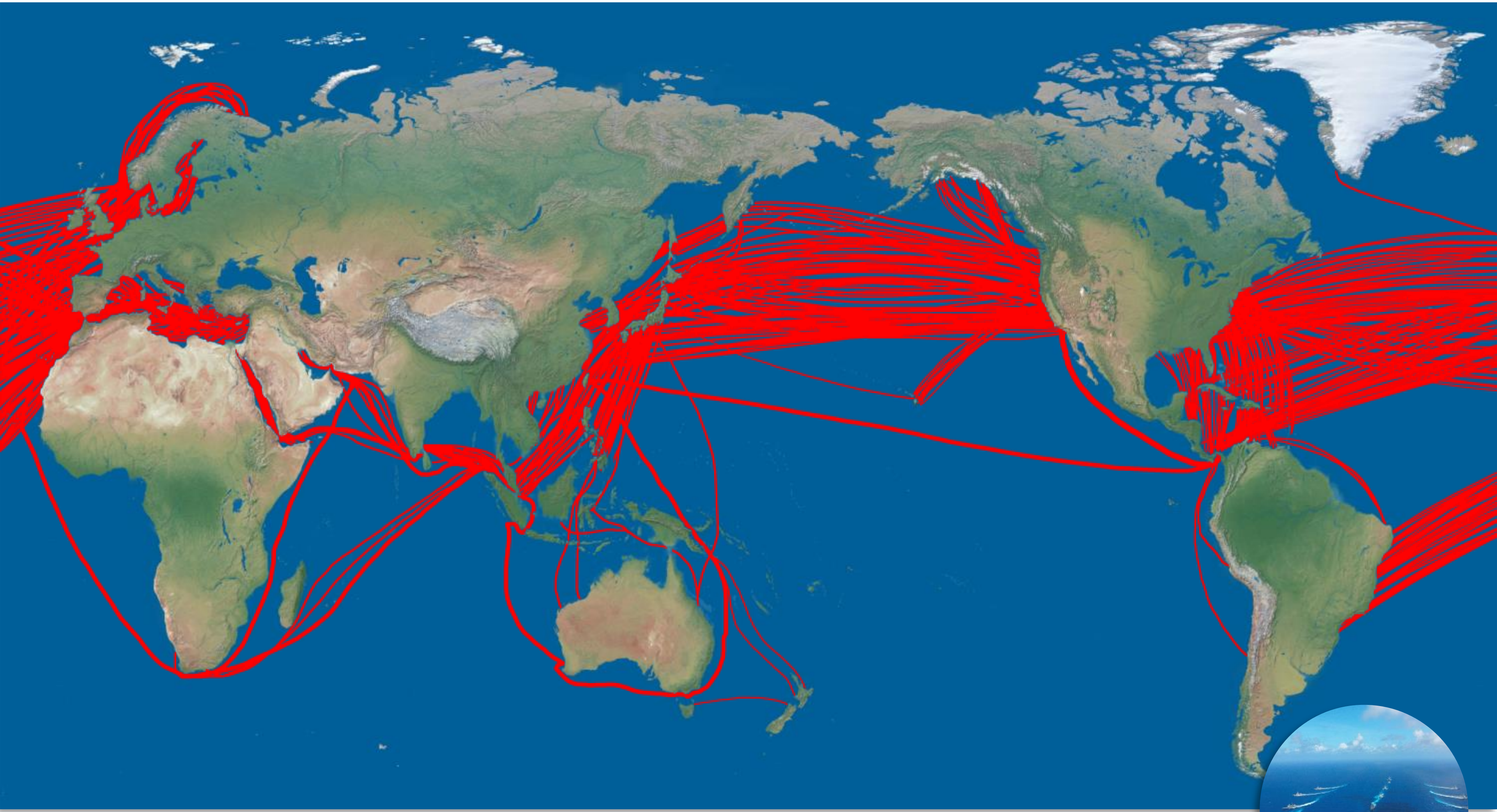
VADM Paul Grosklags, Commander, NAVAIR

Day in the life of an SE dealing with PMs

Framing the Challenge

Life Has Been Good!

Sea Lanes Remain the Lifeblood of Our Economy

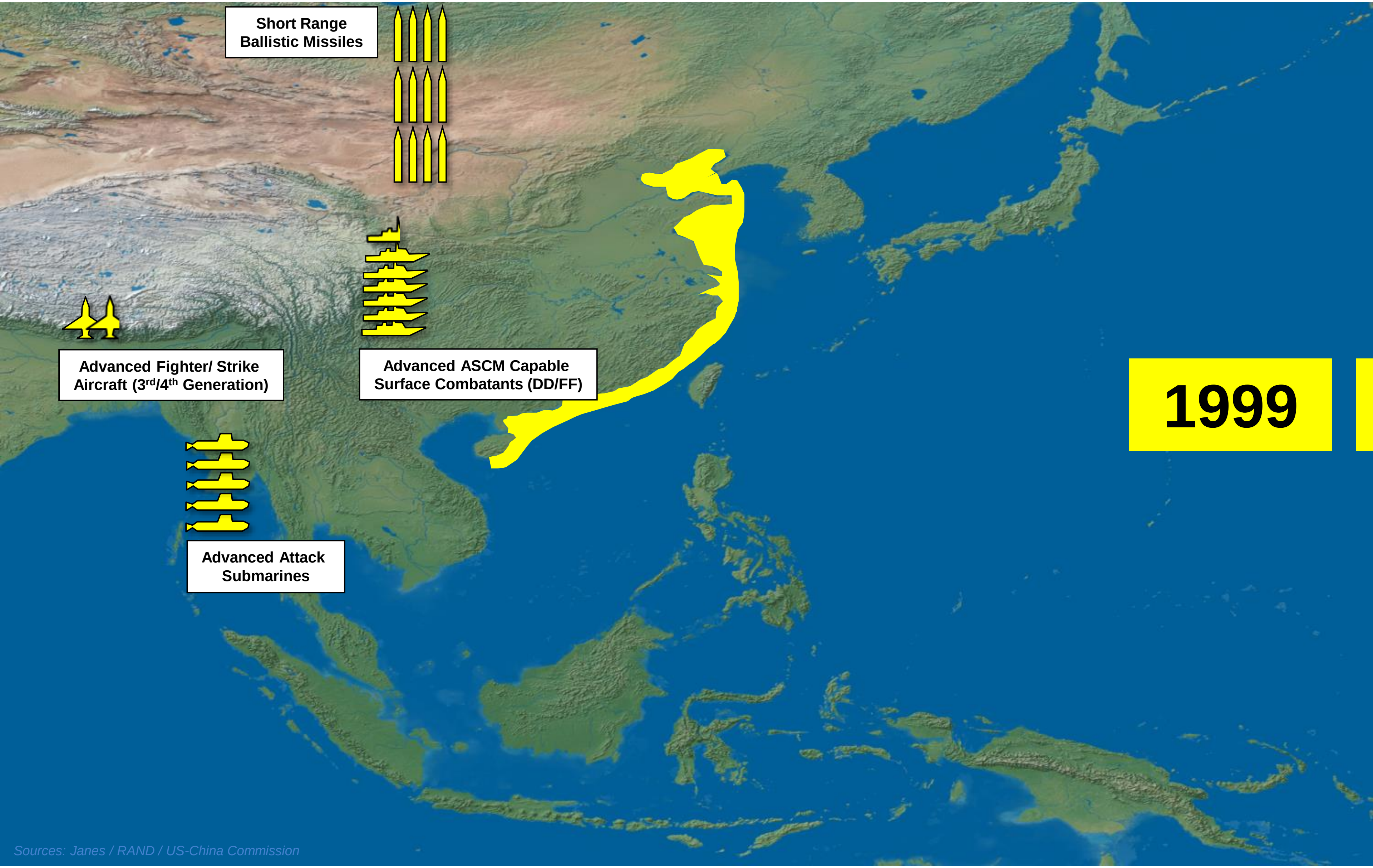


90% of global trade by **volume** / **70%** of global trade by **value**
98% of telecoms traffic

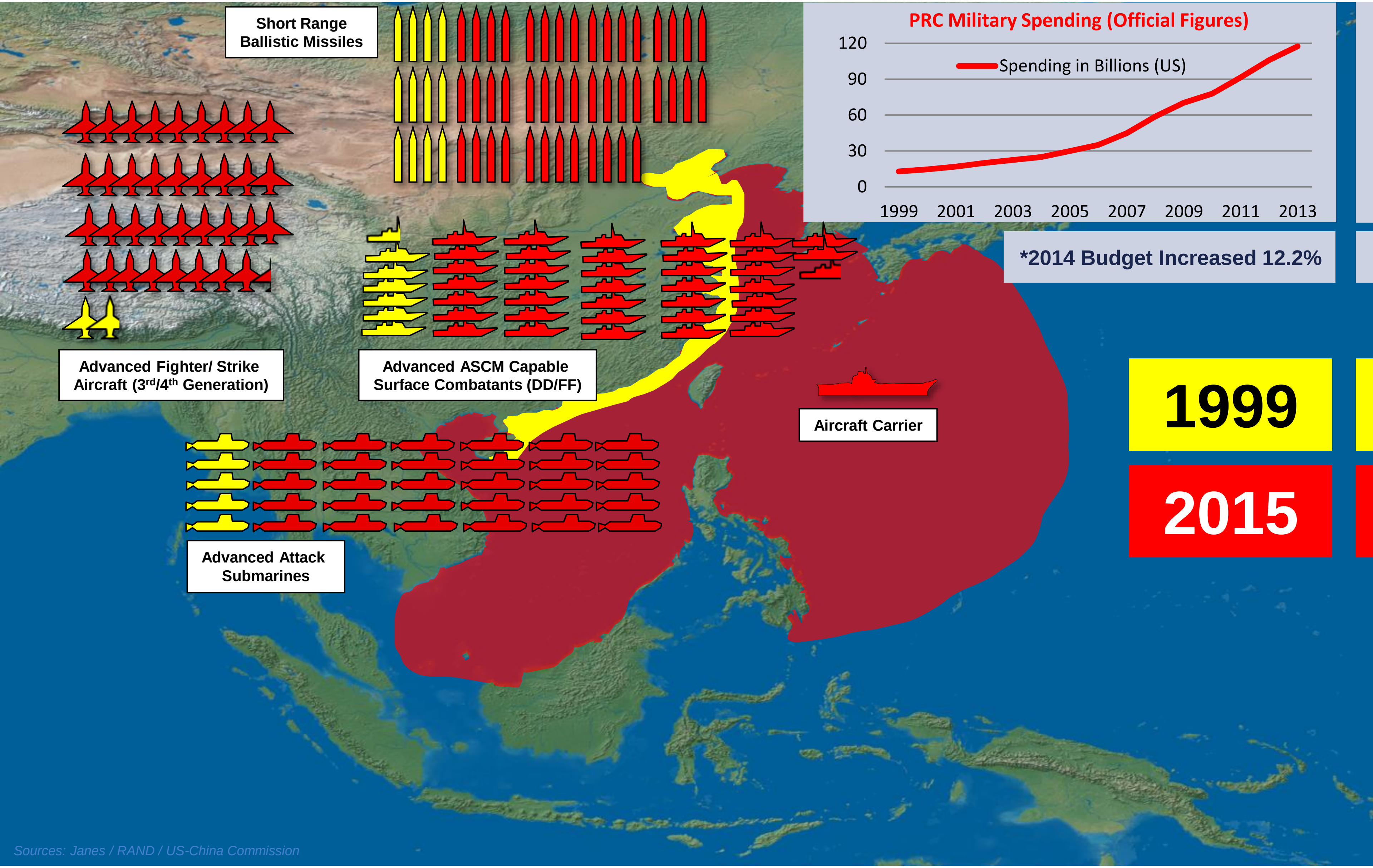
Competition is Back

Distribution Statement A:
Approved for public release; distribution unlimited PR# 2017-928

Changing Environment

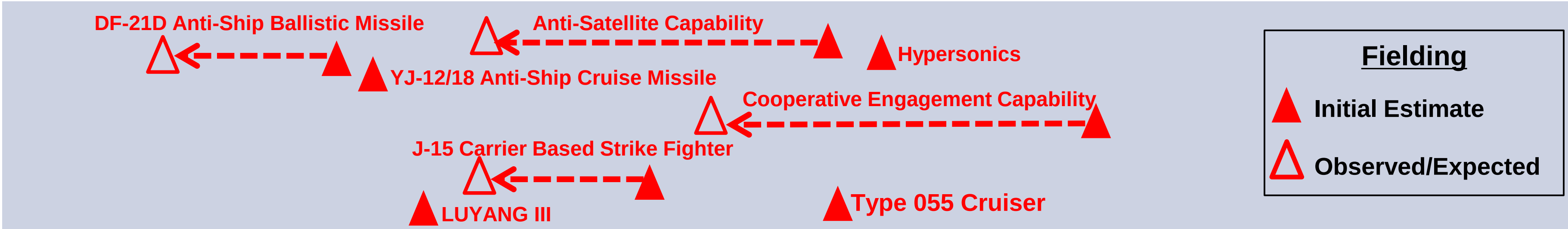


Changing Environment

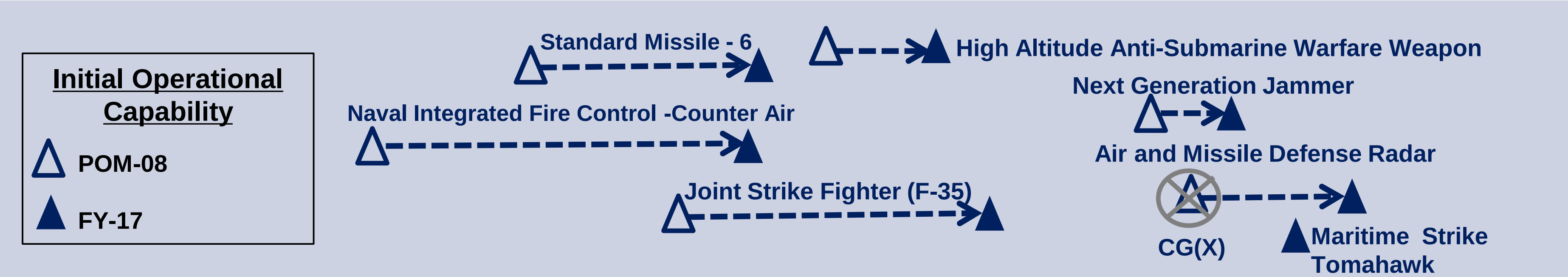


Distribution Statement A: Approved for public release; distribution unlimited PR# 2017-928

USN and PLA(N) Capability Fielding Trends



We're Slower!



USN Warfighting Advantage has Steadily Eroded

CNO's Challenges to all Flag/SES

5 Key Points

- Must be competitive ➡ Existential Threat ➡ No #2
- Think Strategically ➡ Critical Thinking

- Going Digital
- Outcome / Product Oriented ➡ Vice Process

- Sense of Urgency ➡ Should be Uncomfortable

"If It's Not Making the Fleet More Lethal – Stop Doing It!"

NAVAIR Response

Commander's Intent – *Remains Unchanged*

- Increase Speed of New Capabilities to Fleet
- Increase Readiness

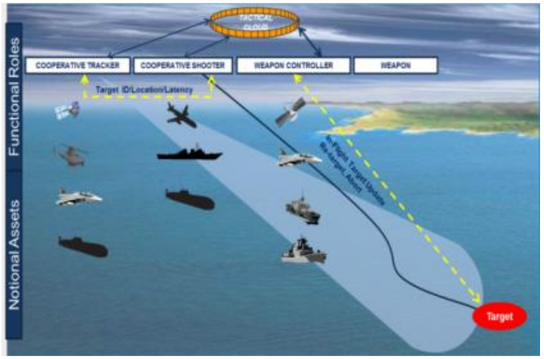
Strategic Initiatives – *Focus on Speed*

- Capabilities Based Acquisition – *Rapid delivery of integrated capabilities*
- Sustainment Vision 2020 – *Predictive, integrated sustainment operations*
- Digital Business Operations – *Integrated business systems "apps" at the desktop*

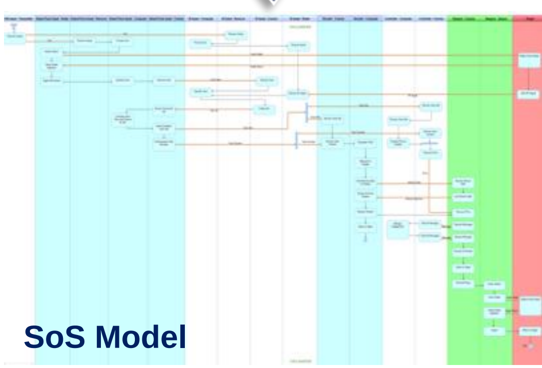
Accelerating delivery of fully integrated capabilities which are designed, developed, and sustained in a Model Based Digital Environment IS a Systems Engineering challenge

Capabilities Based Acquisition

Digital Thread Enables Rapid Delivery of Integrated Capabilities



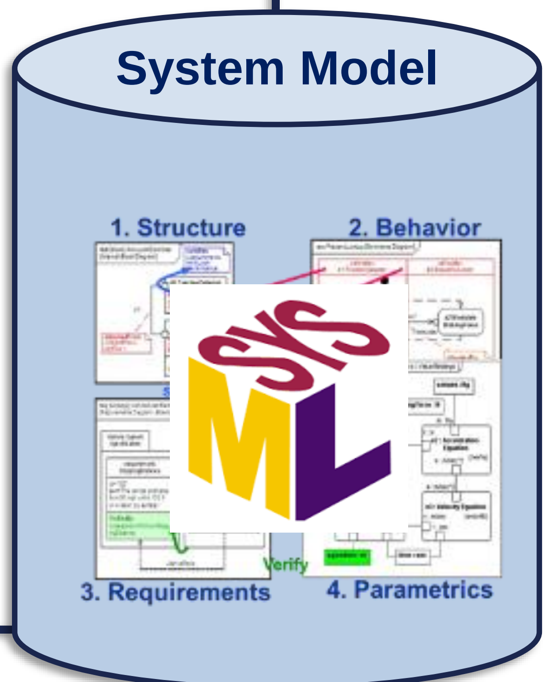
Integrated Warfare Analysis establishes CONEMPS, Effects-Chains, required attributes



CONEMPS and Effects Chains are modeled at the System of Systems (SoS) level

Digital Linkage

System models form "Constructive" basis for LVC M&S environment



Systems are developed in a Model-Based environment (SE Transformation)

Enabling Capabilities-Based T&E

Constructive	Virtual	Live
DIGITAL MODELING	HARDWARE IN THE LOOP	FLIGHT TEST

DIGITAL MODELING

HARDWARE IN THE LOOP

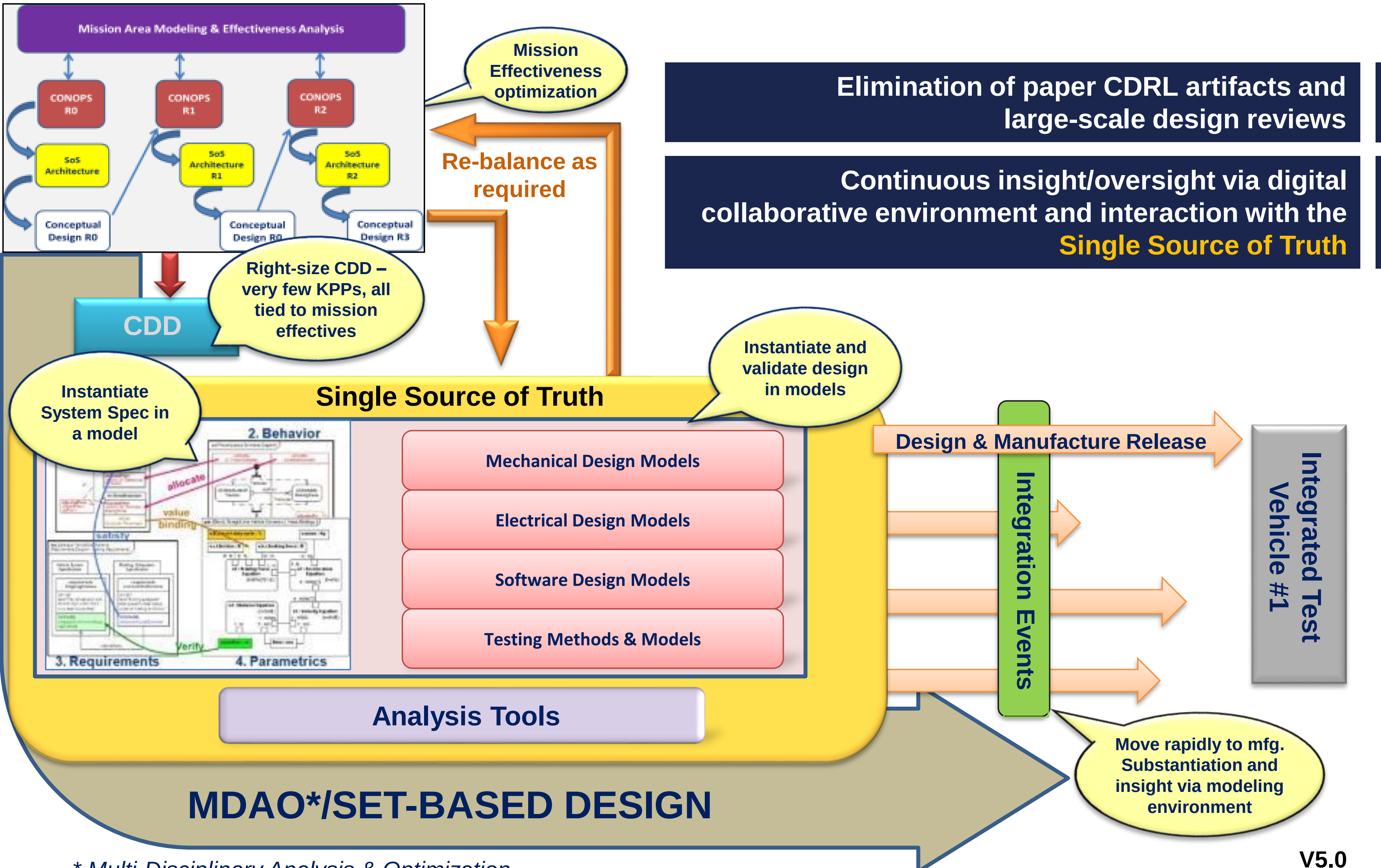
FLIGHT TEST

INTEGRATION LABORATORY

INSTALLED SYSTEMS TEST FACILITY

LVC-based training required for Fleet integrated ops

SET Framework



** Multi-Disciplinary Analysis & Optimization*

V5.0

Execution Framework

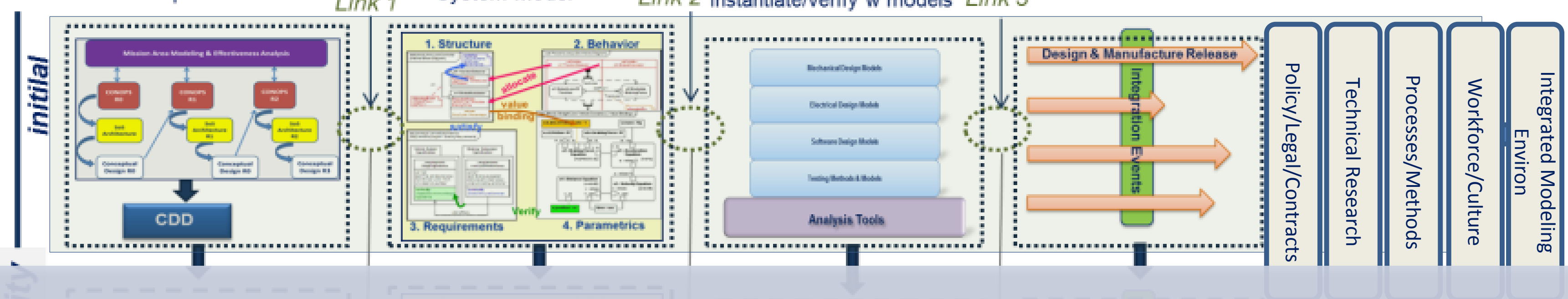
ELEMENT 1
Effectiveness Analysis
CDD optimization

ELEMENT 2
Instantiate Spec in
System Model

ELEMENT 3
Develop Initial Balanced Design
via MDAO/SBD
Instantiate/verify w models

ELEMENT 4
Design & Mfg Release
Collaborate via IDE

Functional Areas



SET Task Framework

Enablers

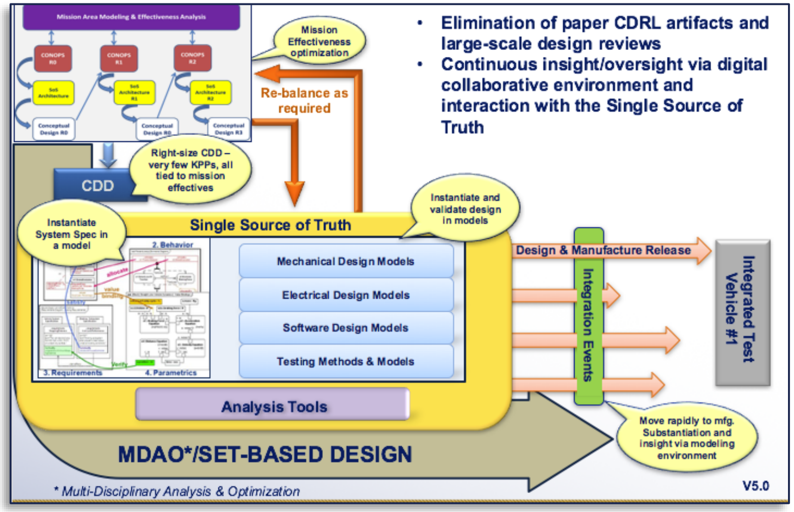
Jaime Guerrero, SET Lead **David Meiser, SET Action Officer**

SET Research Team *(Blackburn)*	**Modeling Env'nt Team** *(Fields)*	**Workforce/Culture Team** *(Carlson)*	**Process & Methodology Team** *(Chamberlain/Polakovics)*	**Policy, Contract, Legal Team** *(Vacant)*	**SET Framework Links** *(S. Raley)*

Each Element requires work in the 5 Functional Areas in order to reach "Full Maturity"

Surrogate System Experiment

- Simulate Execution of SET Framework
- Use UAV scenario developed in SERC models
  - Combine SysML models already in development – requirements, with functional and logical views
  - Use MDAO of parametrics for some KPPs
    - Consider NATO example
    - Characterize objectives and thresholds
  - Create a model-based contract simulating RFP / SOW



- Use commercial organization to simulate industry organization
  - Refinement of SysML models to reflect corrections / innovations with physical allocation views
  - Integrate with multi-physics-based Initial Balanced Design
  - Simulate continuous virtual reviews and derive new objective measures for assessing maturing design
- Simulate source selection based on dynamic models and simulations

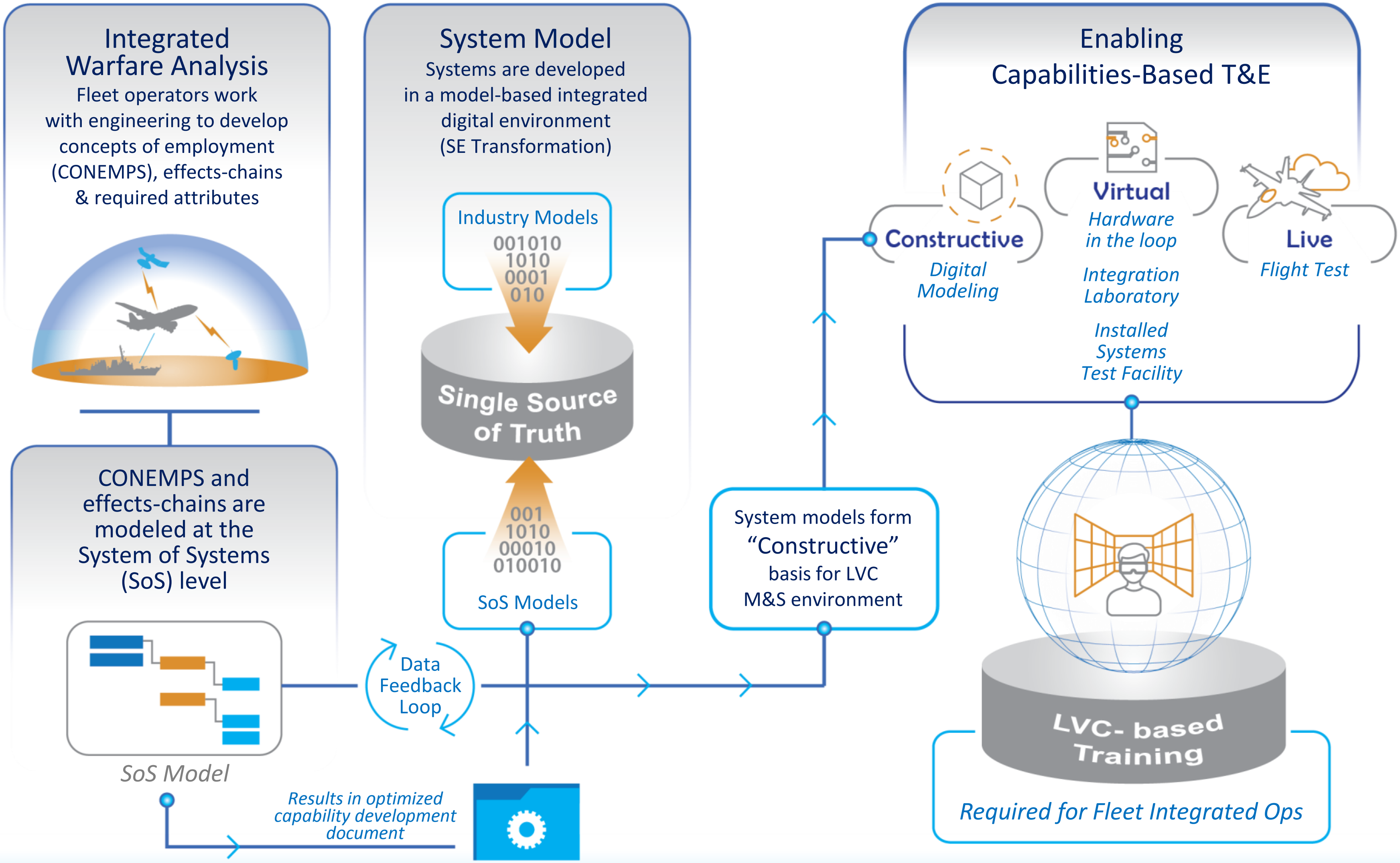
Industry-Government Partnership

- SET applies to both Government and Industry
- Government must reassess its role in the acquisition process and the methods for executing that role
  1. Criteria for gov't involvement / oversight (not every decision)
  2. If involved, must be on developer's timeline
  3. Must bring value to the decision – not just positional authority
- Industry must fully leverage advances in HPC-enabled models and participate in establishing a collaborative, integrated digital environment which enables continuous interaction

For More Information, Contact:

Mr. Dave Cohen, Director Systems Engineering
(301) 757-5542
david.cohen@navy.mil

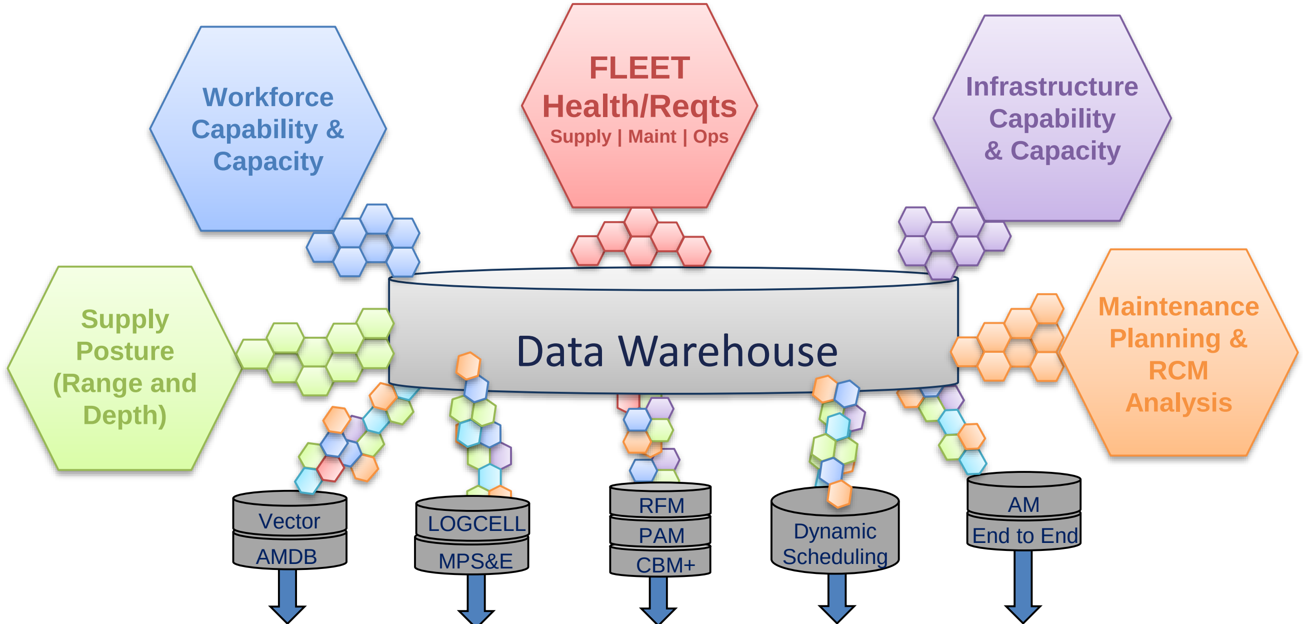
Capabilities Based Acquisition



Integrated Digital Environment accelerates delivery of operationally relevant capabilities

Sustainment Vision 2020 – What it Looks Like

RAW DATA



APPLICATIONS / TOOLS

ANALYSIS

STATUS-TRENDS-PREDICTIONS

FLEET DECISIONS
FLEET SUPPORT

Optimization and Prioritization of Resources to Meet Fleet Needs…
Maintenance Planning
Supply Support
Workforce
Facilities

Universal Information
Faster Decision Making
Predictive Sustainment Planning
Reduced Cost
Increased Readiness

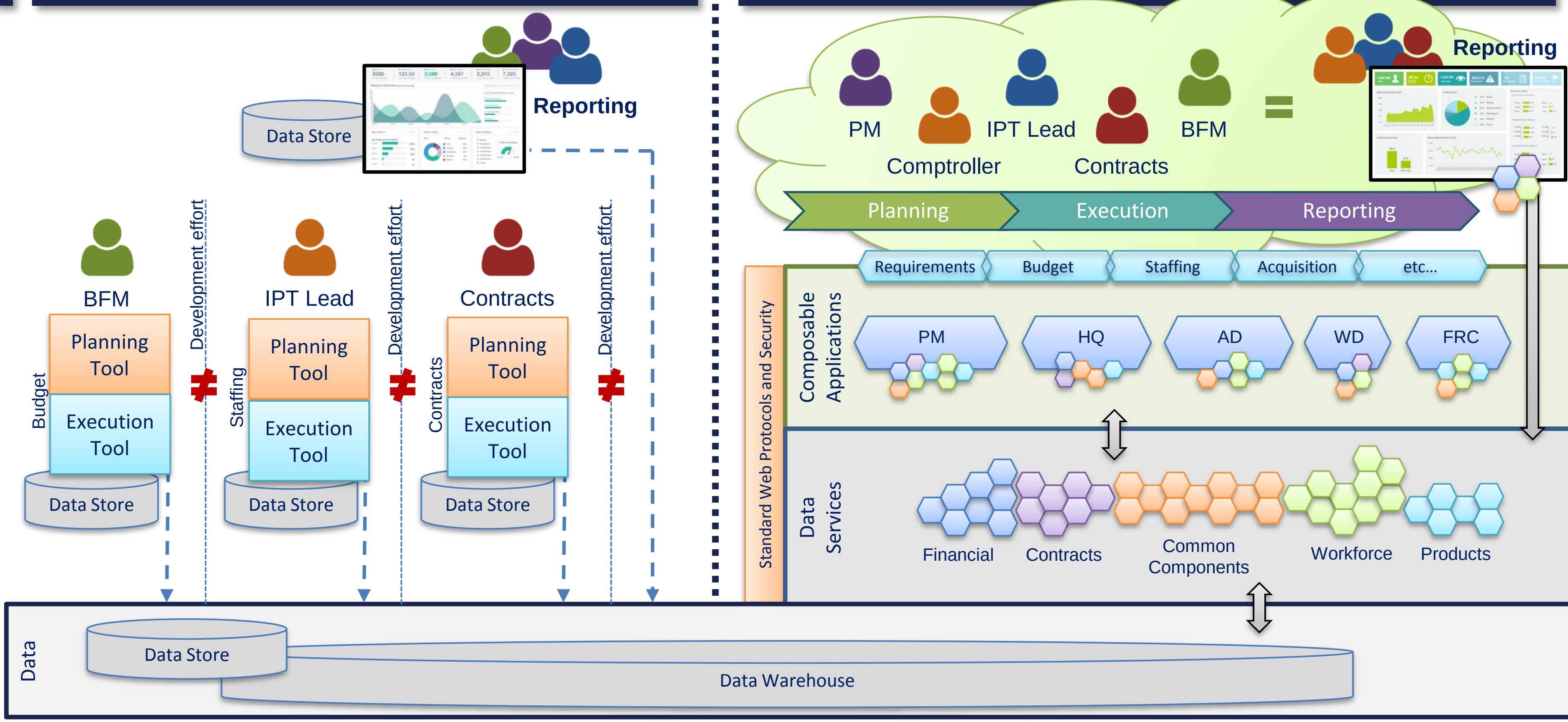
Digital Transformation: Business Operations

Today: Monoliths in Silos

- Applications built in silos
- Data duplicated in tools causing manual re-entry
- Data locked in tools preventing ease of re-use
- Application changes slow and costly
- Functionality duplicated across tools causing inconsistencies and difficulty in coordinating business process changes
- Can't tailor to support unique process across business units
- Similar functionality reinvented over and over again at great cost

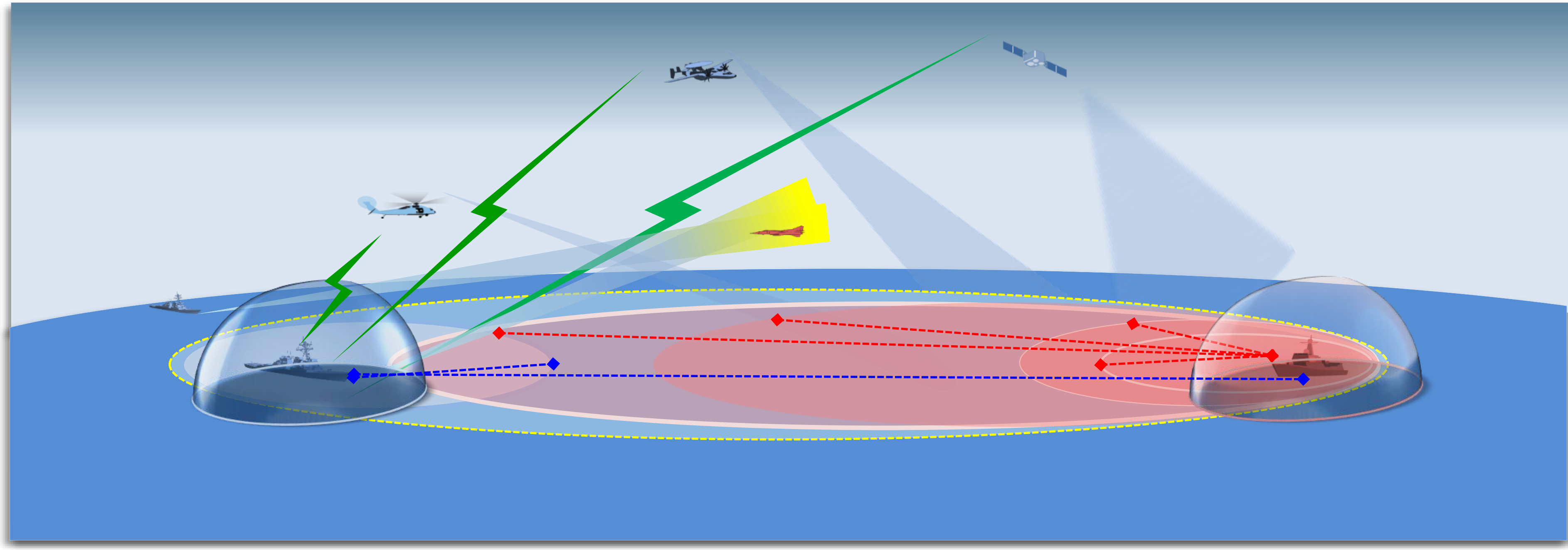
Tomorrow: The Composable Business

- Infrastructure enables tailored applications while maintaining consistent core business rules and data
- Applications "composed" from reusable services
- Consistency of Data and Business Rules across Business Operations
- Agility in supporting rapid Business Process changes
- Lightweight services with short development lifecycle
- Individual Services "owned" by Authoritative Competency



Distribution Statement A:
Approved for public release; distribution unlimited PR# 2017-928

USN vs PLA(N) Capability Fielding



We're Being Out-Sticked

USN Warfighting Advantage Against PLA(N) has Steadily Eroded

CLEARANCE REQUEST FOR PUBLIC RELEASE OF DEPARTMENT OF DEFENSE INFORMATION

(See Instructions on back.)

(This form is to be used in requesting review and clearance of DoD information proposed for public release in accordance with DoDD 5230.09.)

TO: *(See Note)* **Chief, Office of Security Review, 1155 Defense Pentagon, Washington, DC 20301-1155**

Note: Regular mail address shown above. For drop-off/next day delivery, use:
Room 12047, 1777 North Kent Street, Rosslyn, VA 22209-2133

1. DOCUMENT DESCRIPTION

a. TYPE Brief	b. TITLE **"Best Practices for the Architecture, Design, and Modernization of Defense Models and Simulations" (Brief)**
c. PAGE COUNT 17 Pages	d. SUBJECT AREA DoD Modeling & Simulation (M&S)

2. AUTHOR/SPEAKER

a. NAME *(Last, First, Middle Initial)* Citizen, Jesse J., Jr.	b. RANK CIV	c. TITLE Director, DMSCO
d. OFFICE Defense Modeling & Simulation Coordination Office (DMSCO)		e. AGENCY USD(AT&L)/ASD(R&E)/SE/DMSCO

3. PRESENTATION/PUBLICATION DATA *(Date, Place, Event)*

Date of event: Oct 23-Oct 26, 2017
Place: Waterford at Springfield, 6715 Commerce Street, Springfield, VA 22150
Event: 20th Systems Engineering (SE) Conference (http://www.ndia.org/events/2017/10/23/20th-systems-engineering-conference)

4. POINT OF CONTACT

a. NAME *(Last, First, Middle Initial)* Mock, Sherrel W or Robinson, David A - Public Affairs Email address: osd.msco.pao@mail.mil	b. TELEPHONE NO. *(Include Area Code)* 571-372-6787

5. PRIOR COORDINATION

a. NAME *(Last, First, Middle Initial)*	b. OFFICE/AGENCY	c. TELEPHONE NO. *(Include Area Code)*
SLIDES ONLY NO SCRIPT PROVIDED		

CLEARED
For Open Publication
Oct 02, 2017
2
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

6. REMARKS This brief follows an abstract that supports a continuing effort to share M&S information with M&S practitioners attending the SE conference. DOPSR cleared the abstract on May 15, 2017 (Case #17-S-1721). Most slides have been previously cleared – respective case numbers are annotated. The USD(AT&L), by charter (paras 3 & 3.35 of DoDD 5134.01), is responsible for all matters relating to DoD modeling and simulation. The DMSCO is the OSD office responsible for supporting the USD(AT&L) in the execution of his M&S responsibilities. We believe the information is unclassified and that it is ready for public release. From DMSCO's perspective, this brief does not violate any security concerns.

*NOTE: Request scanned .pdf copy of DOPSR-stamped DD Form 1910 be sent to email address in Block 4a, above. **If the DOPSR-stamped hard copy is returned, please mail to POC in blocks 4a & 4b above at DMSCO, 4800 Mark Center Drive, Suite 16E08-08, Mailbox 46, Alexandria, VA 22350-3600.***

7. RECOMMENDATION OF SUBMITTING OFFICE/AGENCY

a. THE ATTACHED MATERIAL HAS DEPARTMENT/OFFICE/AGENCY APPROVAL FOR PUBLIC RELEASE *(qualifications, if any, are indicated in Remarks section)* AND CLEARANCE FOR OPEN PUBLICATION IS RECOMMENDED UNDER PROVISIONS OF DODD 5230.09. I AM AUTHORIZED TO MAKE THIS RECOMMENDATION FOR RELEASE ON BEHALF OF:

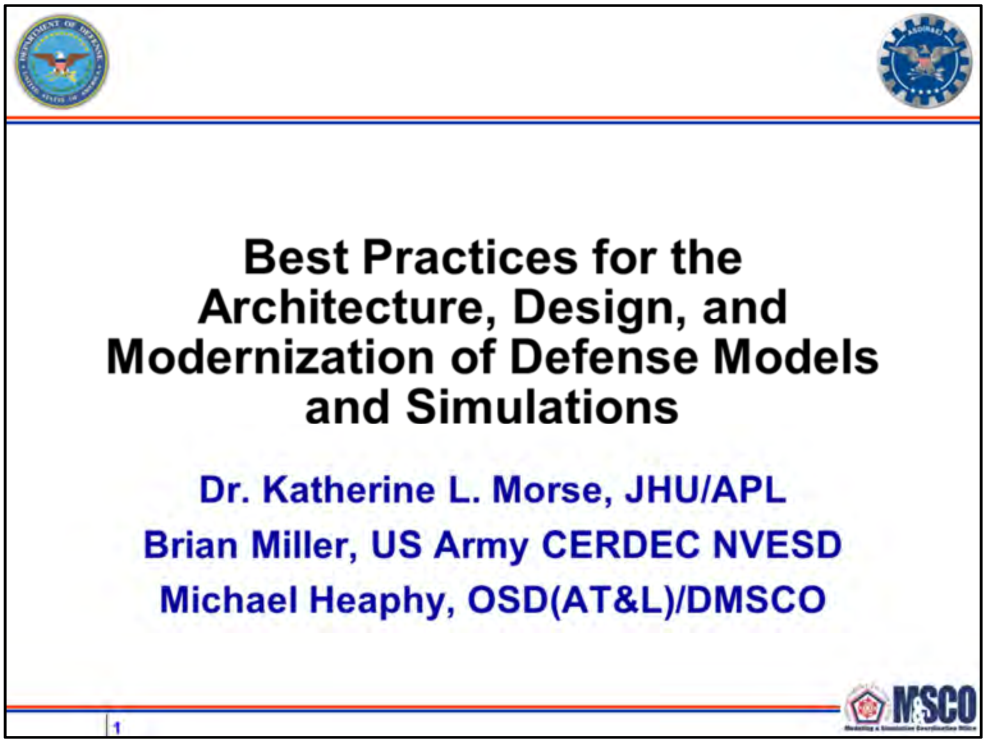
Defense Modeling & Simulation Coordination Office (DMSCO)

b. CLEARANCE IS REQUESTED BY 20171006 DAU *(YYYYMMDD)*.

c. NAME *(Last, First, Middle Initial)* Yu, Leigh G.	d. TITLE Deputy Director, DMSCO
e. OFFICE Defense Modeling & Simulation Coordination Office (DMSCO)	f. AGENCY USD(AT&L)/ASD(R&E)/SE/DMSCO
g. SIGNATURE	h. DATE SIGNED *(YYYYMMDD)* DAU 20170527

DD FORM 1910, JAN 2006 PREVIOUS EDITION MAY BE USED. Adobe Professional 8.0

17-S-2666



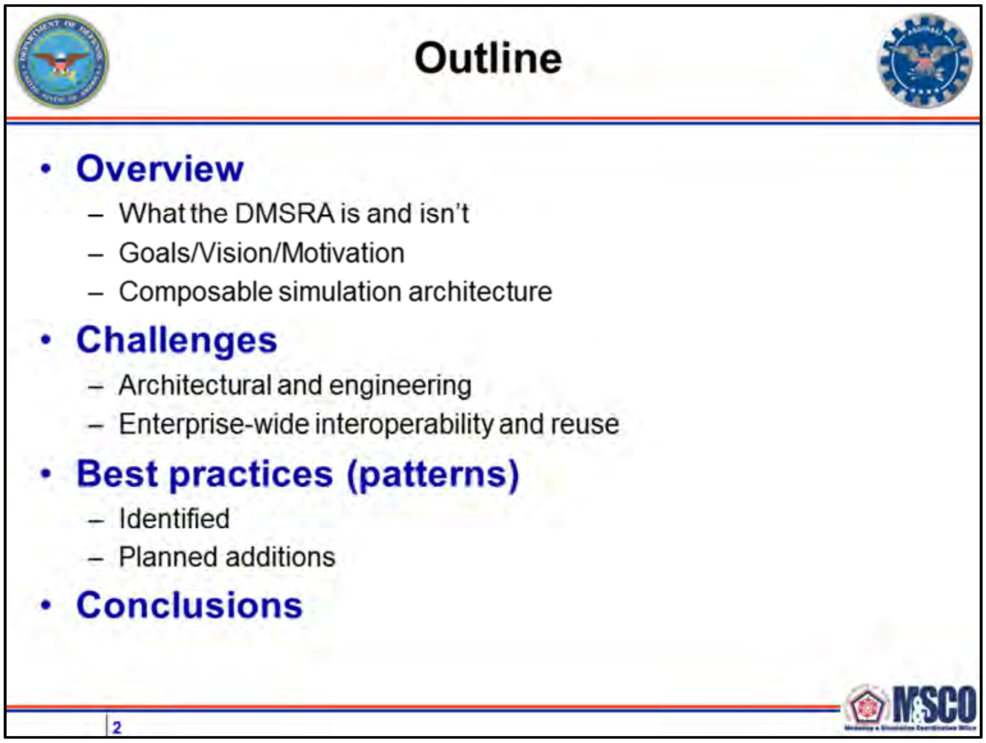
SLIDES ONLY

NO SCRIPT PROVIDED

17-S-2666

Best Practices for the Architecture, Design, and Modernization of Defense Models and Simulations

Dr. Katherine L. Morse, JHU/APL
Brian Miller, US Army CERDEC NVESD
Michael Heaphy, OSD(AT&L)/DMSCO


Outline
• Overview
– What the DMSRA is and isn't
– Goals/Vision/Motivation
– Composable simulation architecture
• Challenges
– Architectural and engineering
– Enterprise-wide interoperability and reuse
• Best practices (patterns)
– Identified
– Planned additions
• Conclusions
2
M&SCO

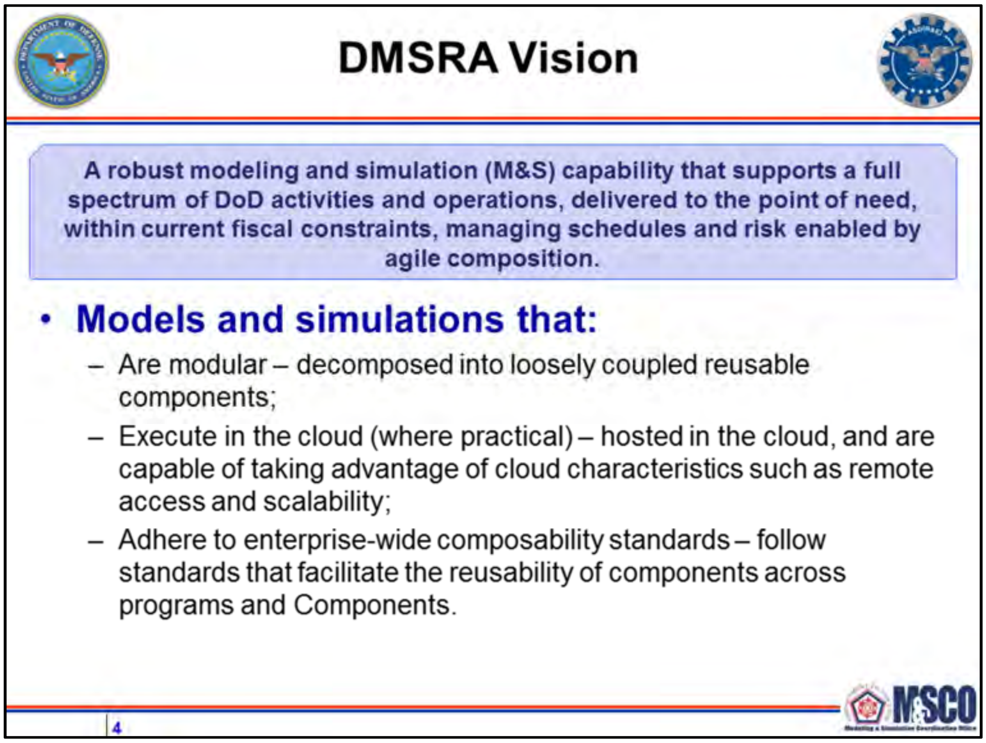
New slide

Overview

- **The DMSRA is NOT a solution architecture.**
- **It establishes a vision for Defense M&S:**
  - that leverages emerging technologies, and enterprise services;
  - to promote reuse and interoperability.
- **The DMSRA provides broadly applicable guidance.**
  - It captures principles, standards, and best practices for simulation architects and engineers to align on the vision.
  - It is not mandatory.

3

New slide



This slide was cleared in DOPSR Case #17-S-2193, slide 3:

DMSRA Motivation:

The Federal Government and DoD have IT strategies promoting the adoption of cloud computing

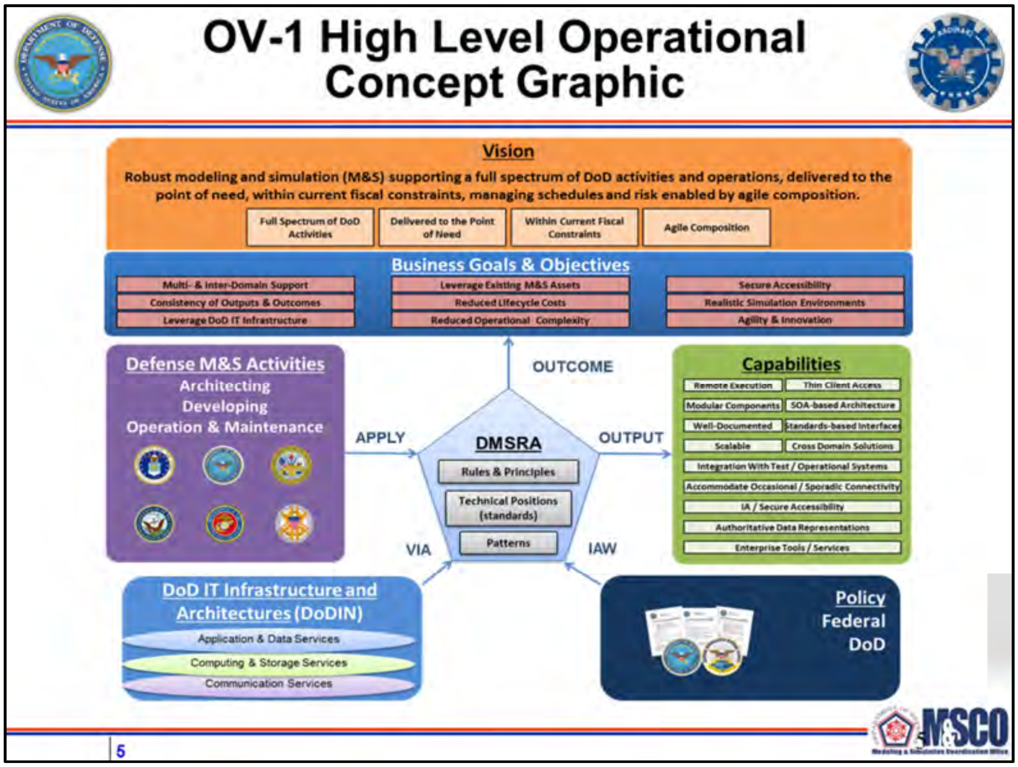
- •Initiatives are already under way such as the the Joint Information Environment (JIE) which will change how the department does IT business
- •The M&S community must prepare for the coming changes

Technologies such as cloud computing and service-oriented architecture (SOA) can provide significant opportunities

- •To improve accessibility and agility
- •While reducing operating and maintenance costs

These technologies inherently promote reusability

- •By coordinating their implementation across the department we can
  - Reduce development time and cost
  - Increase simulation accuracy through component reuse



[Note: This figure was cleared by DOPSR on June 6, 2016 (Case #16-S-2052, page 5 of 12)]

DMSRA Structure:

Strategic Purpose

Goals and objectives of the DMSRA; specific purpose of and the problem(s) to be addressed by the DMSRA.

Principles

High-level foundational statements of stakeholders, rules, and values that drive technical positions and patterns.

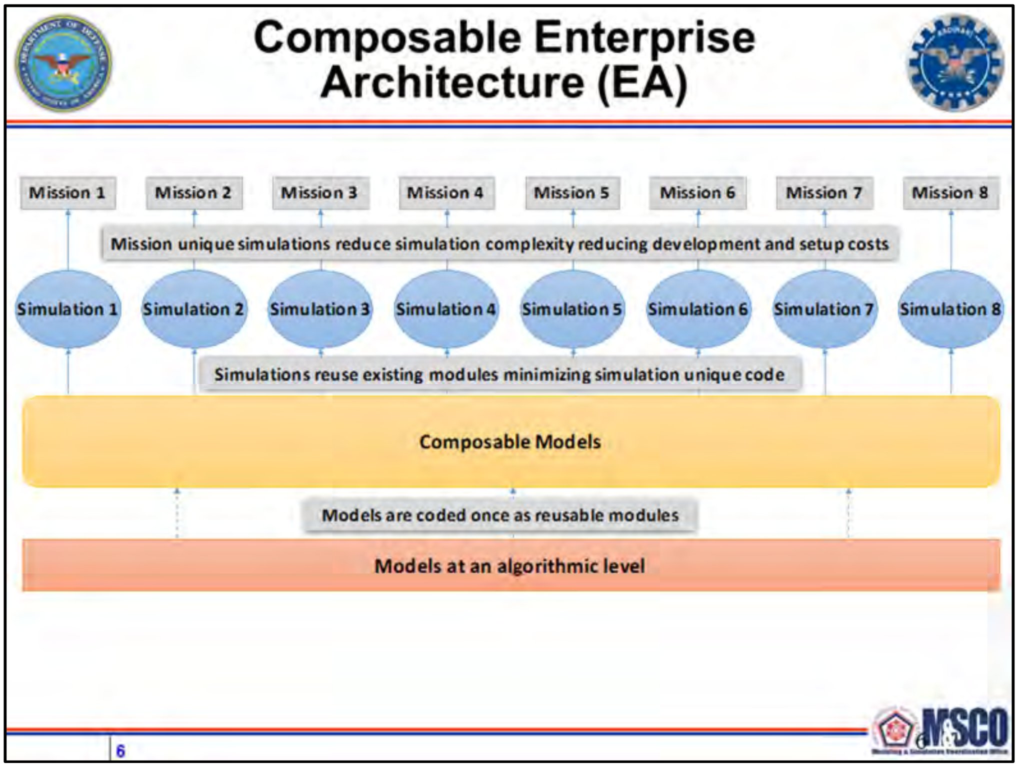
Technical Positions

Technical guidance and standards, based on specified principles that need to be followed and implemented as part of the solution.

Patterns (Templates)

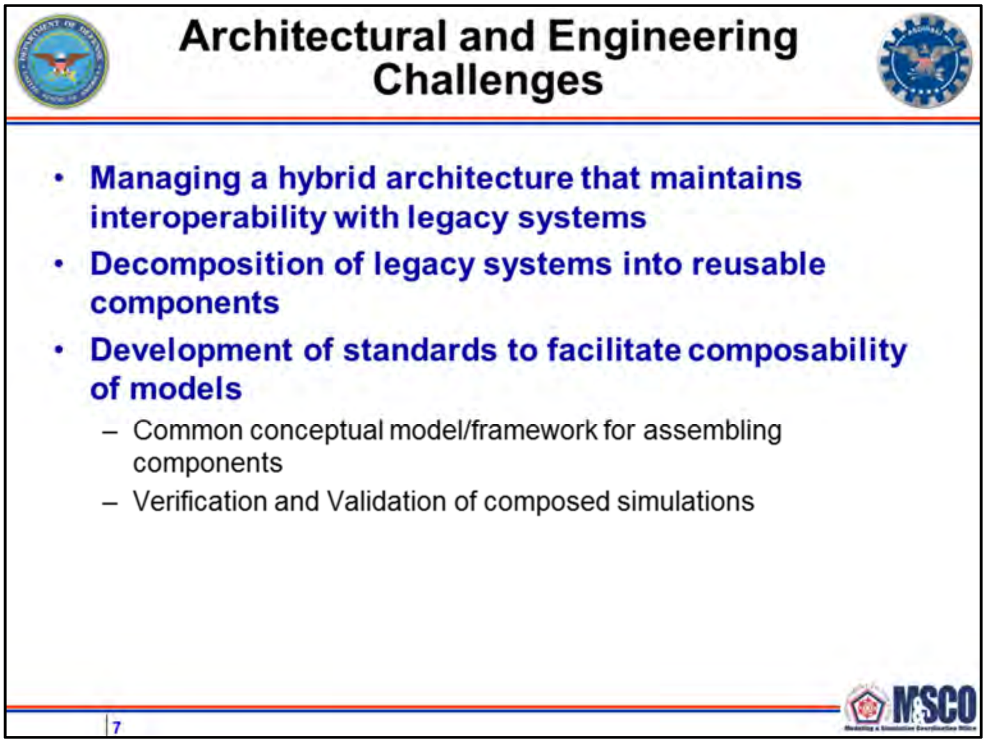
Generalized architecture representations (viewpoints, graphical/textual models, diagrams, etc.) that show relationships between elements and artifacts specified by the technical positions and encourage adherence to common standards, specifications and patterns.

Vocabulary

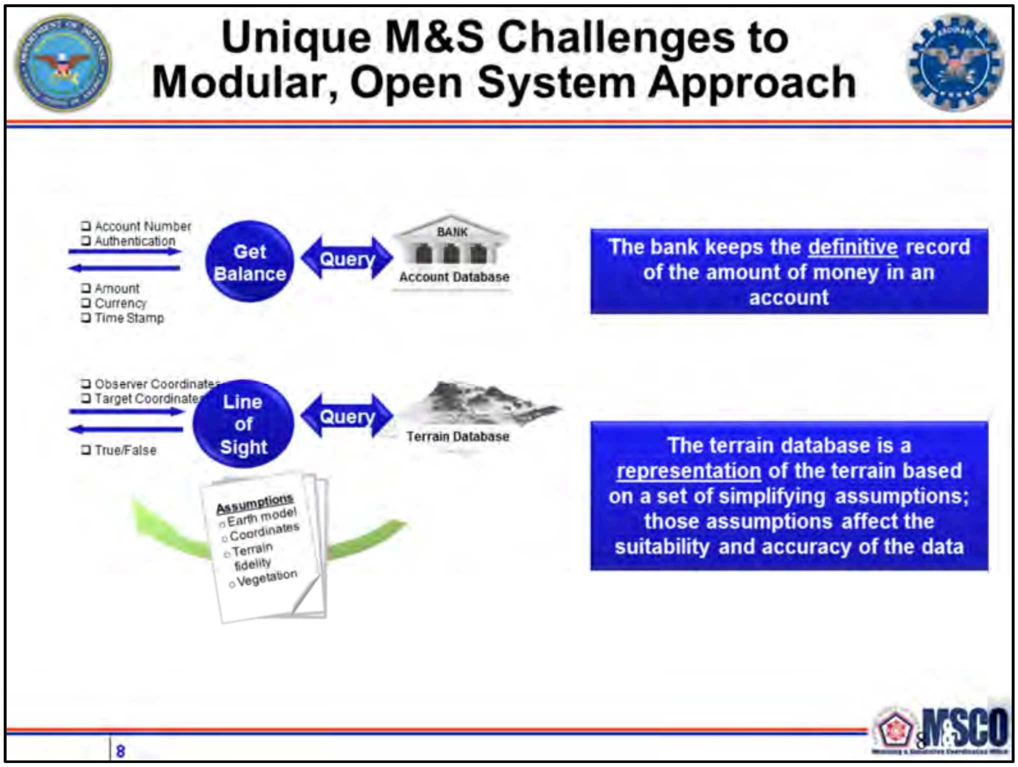


[Note: This figure was cleared by DOPSR on June 6, 2016 (Case #16-S-2052, page 9 of 12)]
Notes from: table cleared by DOPSR on June 6, 2016 (Case #16-S-2052, page 9 of 12):
Advantages:

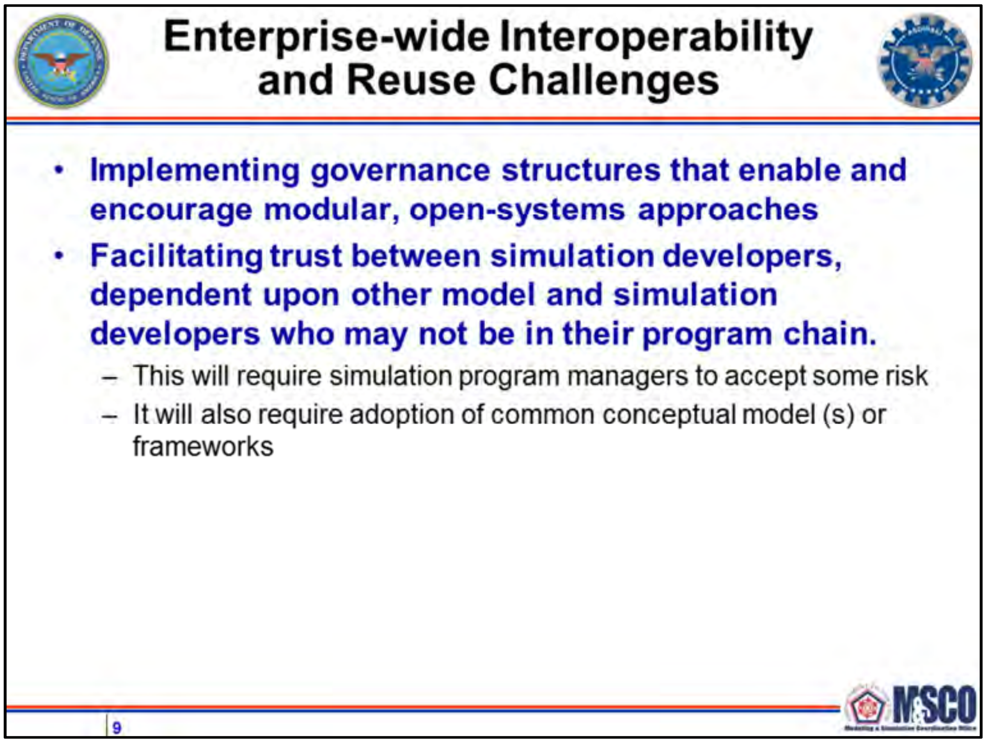
- Models are coded once, reducing development time and cost
- Easy to replace models with newer versions that use the same interface
- Smaller simulations should lead to easier use and reduced maintenance costs
- Conducive to cloud computing infrastructure



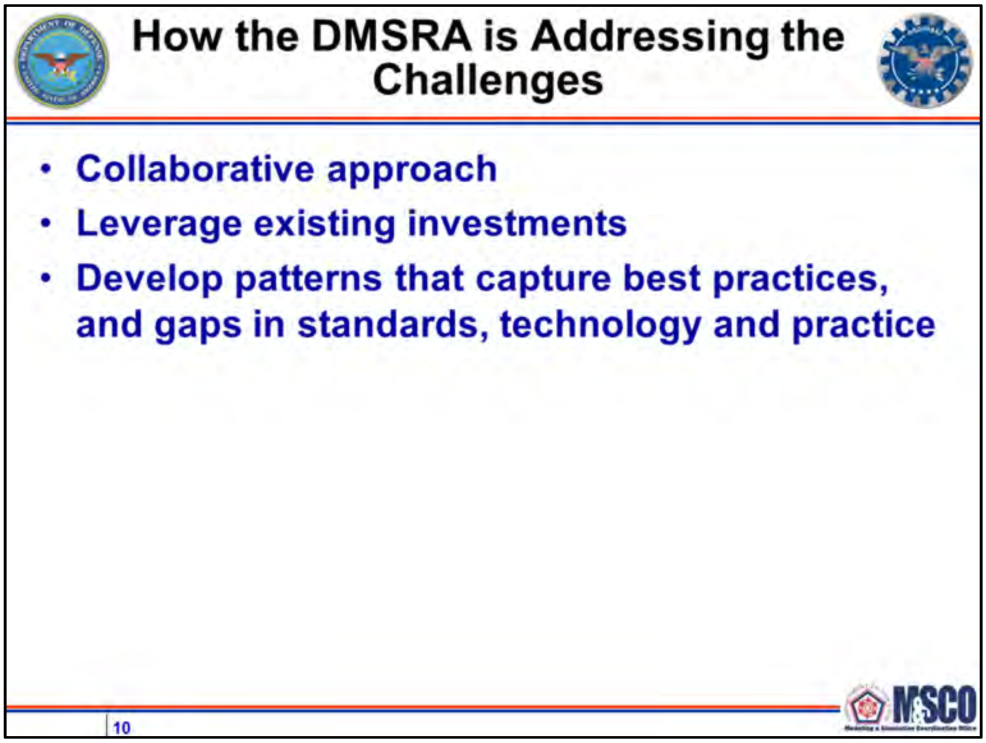
Includes content from table cleared by DOPSR on June 6, 2016 (Case #16-S-2052, page 9 of 12)]



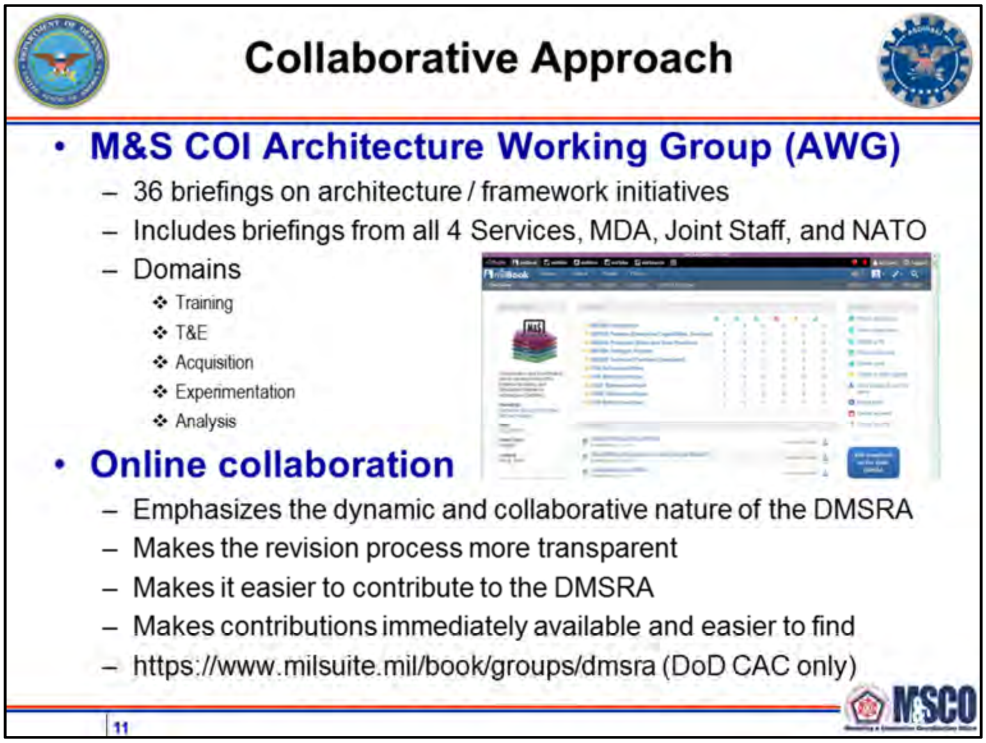
[Note: This slide was cleared by DOPSR (Case #17-S-2610, page 12)]



Includes content from table cleared by DOPSR on June 6, 2016 (Case #16-S-2052, page 9 of 12)]


How the DMSRA is Addressing the Challenges
• Collaborative approach
• Leverage existing investments
• Develop patterns that capture best practices, and gaps in standards, technology and practice
10
MSCO

New slide



[Note: Portions of this slide were cleared by DOPSR on for presentation at I/ITSEC 2016. (case # 16-S-2705, slide 6.)]
[Note: The number of briefings will need to be updated after the SIW to reflect the briefings given at the special session.]

Leveraging Existing Investments

- **The DMSRA effort builds on the Live, Virtual, Constructive Architecture Roadmap (LVCAR) principles:**
  - Do no harm
  - Interoperability is not free
  - Start with small steps
  - Provide central management
- **Other investments and resources leveraged:**
  - Defense M&S Glossary
  - Verification, Validation, and Accreditation (VV&A) Recommended Practices Guide
  - DoD and NATO standards references and tools
  - Services' architecture(s) artifacts and practices

12

[Note: This slide was cleared by DOPSR (case # 16-S-2705, slide 5)]

Patterns: Best Practices and Gaps

- **Extensibility via Patterns**
  - The base document and initial patterns were not sufficiently comprehensive to meet the DMSRA vision
  - Led to the use of modular patterns to extend and evolve the DMSRA with new technologies and associated best practices.
- **DMSRA Pattern Outline:**
  - **Pattern overview:** Frames topic with definitions, technology description, and relevance to the DMSRA
  - **Mapping from Capabilities, and Principles and Rules:** aligns capability with DMSRA principles
  - **Pattern:** Provides a series of questions the user should ask in the process of deciding whether to apply the technology/capability. Documents guidance and best practices for answering the questions in context based on inputs from the AWG.
  - **Technical Positions:** Identifies applicable standards, including DoD adoption status; and standardization gaps
  - **References**

M&SCO

13

[Note: Portions of this slide were cleared by DOPSR (case # 17-S-2610, slide 15)]

Current Patterns Findings (1 of 2)

- **Cloud migration**
  - Lower overall costs to the consumer, because of efficiencies obtained by pooling much of the computing hardware and software;
  - IT functions and increased flexibility because there is no upfront investment in infrastructure required by the end user
- **Service-oriented architecture**
  - The Department of Defense (DoD) Chief Information Officer (CIO) has directed the DoD to leverage commercial SOA technologies to reduce costs and increase flexibility.
  - This pattern aids the user to determine the suitability of an organizational capability for migration to a SOA from technical, programmatic, and domain perspectives.

14

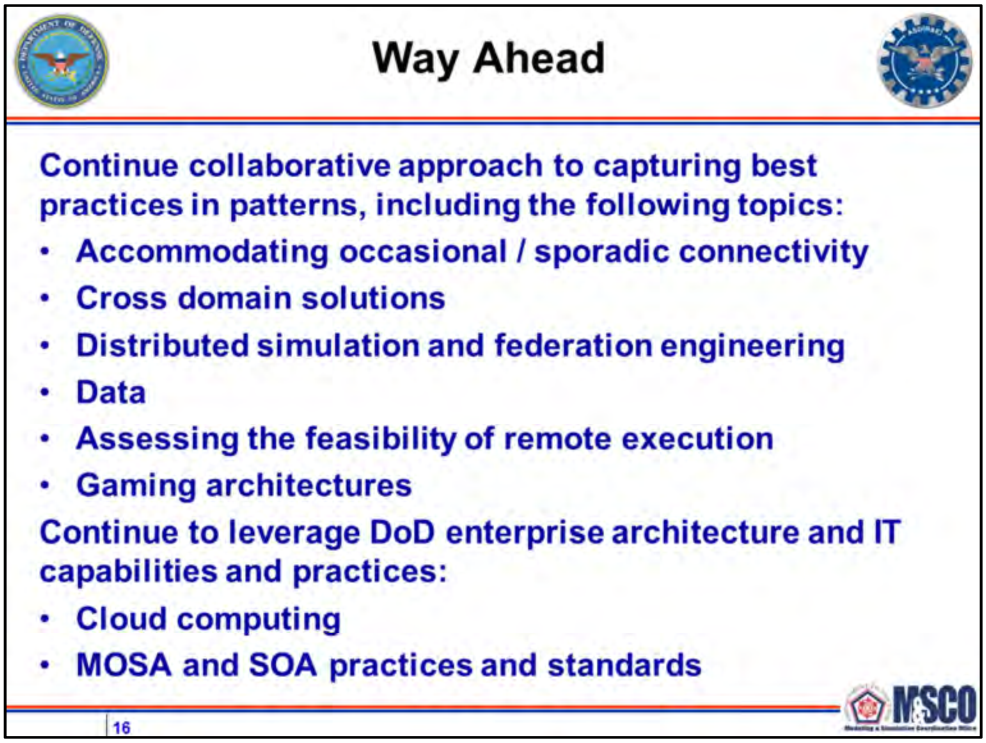
New slide

Current Patterns Findings (2 of 2)

- **Decomposition of simulations into modular components**
  - Although much has been written about modular simulation, there is a gap for M&S-specific standard practices for decomposition.
- **Verification and validation of modular components**
  - Cloud computing considerations: The hardware and operating system the simulation is hosted on are out of the control of the user and may be altered from the configuration used during validation without the user's knowledge.
  - V&V of composed simulations: composition of validated component models does not ensure a valid composed simulation. This is a known gap in standards and practice.

15 MSCO

New slide



[Note: Portions of this slide were cleared by DOPSR (case # 17-S-2610, slide 16)]

QUESTIONS?

17

19701
Leveraging Cybersecurity Tools For Software Safety

Focusing (Some) Static Analysis on Safety-Critical Software

Stuart A. Whitford
Booz Allen Hamilton
20th Annual NDIA Systems Engineering Conference
Springfield, VA
25 October 2017

Agenda

- Some Givens
- Safety versus Security
- General Static Analysis: Dealing with false positives and false negatives
- Targeted Static Analysis: Proving specific properties and assertions
- Coordinating the Efforts
- Conclusion

NOTE: Blue highlighting in this presentation is for ***emphasis.***

Some Givens

[C]ybersecurity applies to weapons systems . . . [and] is a critical priority for the DoD. . . incorporate code reviews and architecture reviews against incremental builds to reduce vulnerabilities in any custom software, including via automated scanning tools (e.g., static analysis).

[*The DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, September 2015]

DoD will continue to assess Defense Federal Acquisition Regulation Supplement (DFARS) rules . . . to ensure they mature . . . in a manner consistent with known standards for protecting data from cyber adversaries, to include standards . . . by the National Institute of Standards and Technology (NIST).

[*The Department of Defense Cyber Strategy*, April 2015]

More Givens

Source code should be periodically reviewed using automated tools or manual spot check for common programming errors . . . as part of the software development QA process.

[NIST Special Publication 800-64 revision 2, *Security Considerations in the System Development Life Cycle*, October 2008]

The Program Manager will integrate ESOH risk management into the overall systems engineering process for all engineering activities throughout the system's life cycle. . . The Program Manager will use the methodology in MIL-STD-882E.

[DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015]

Level of Rigor Tasks [for Software Criticality Index (SwCI) 1/highest] . . . Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.

[MIL-STD-882E, "DoD Standard Practice for System Safety," May 11, 2012]

Software Safety versus Software Security

Software Safety Focus

- Internal data corruption vulnerabilities
- Time critical latency issues
- Vulnerabilities to unintended mistakes in design or implementation

Software Security Focus

- External interface vulnerabilities
- Vulnerabilities to malicious intent

There is some overlap, but the priorities and focus are different.

Software Safety versus Software Security

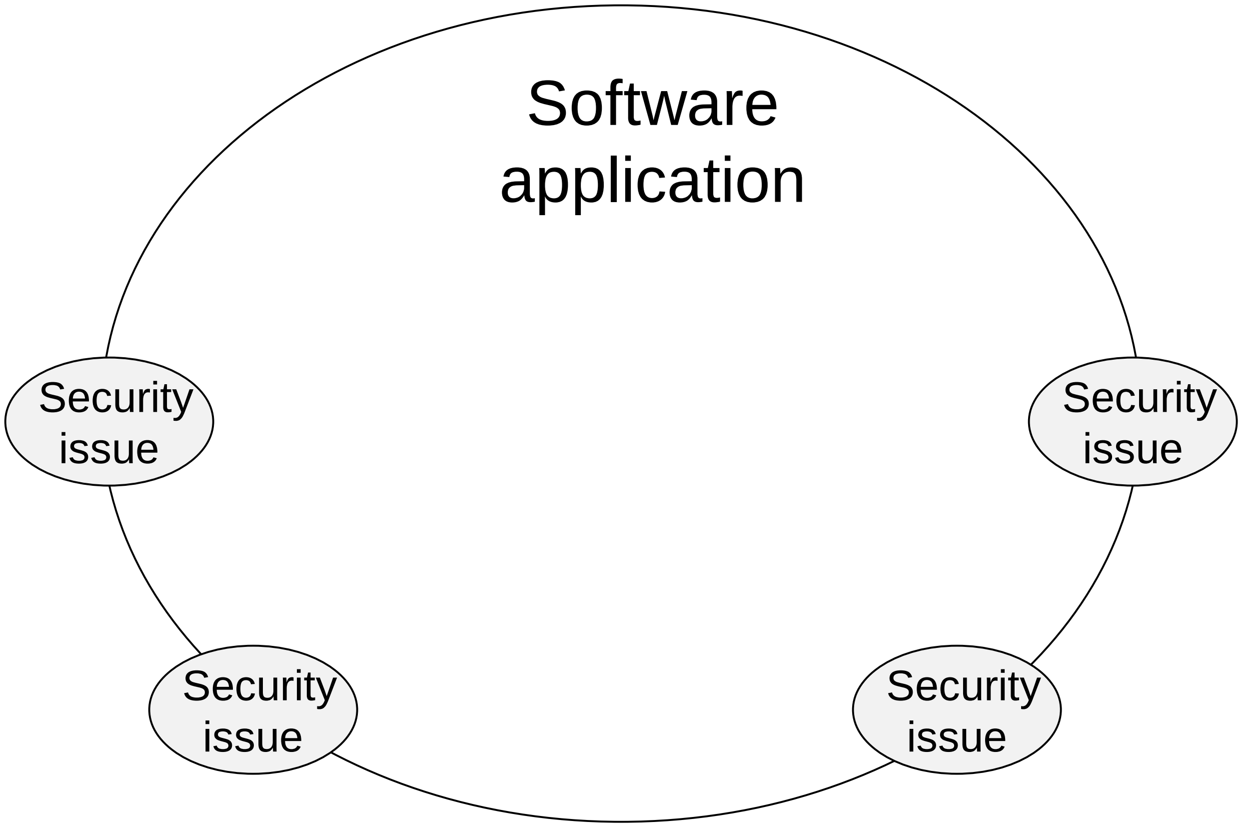
Software Safety Focus

- Race conditions with safety-critical data
- Latency issues with safety-critical response or data update
- Inadequate or erroneous feedback to an operator

Software Security Focus

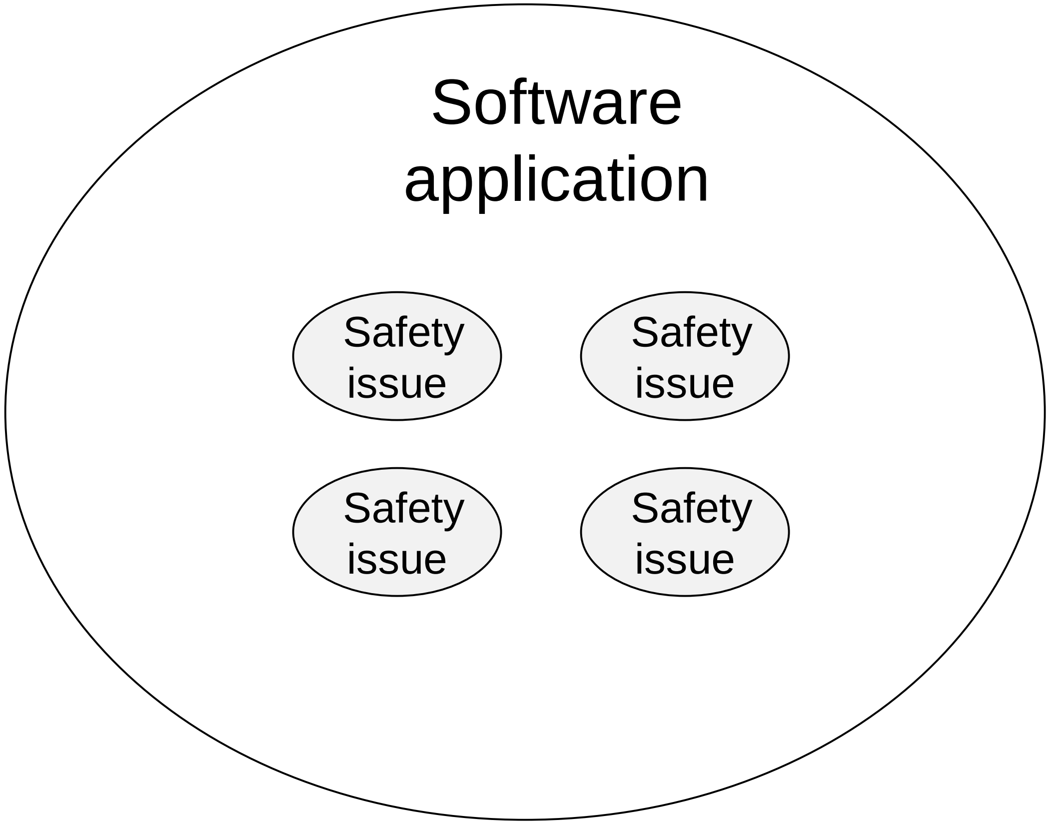
- Missing/incorrect authentication or authorization
- Injection of malicious data or scripts
- Uncontrolled data or buffer overflow

Software Safety versus Software Security



Security issues tend to be at the external interfaces of a software application.

Software Safety versus Software Security



Safety issues tend to be in the core system functionality of a software application.

General Static Analysis:
Dealing with *false positives* and
false negatives

General Static Analysis

- General static source code analysis
  - Flagging programming errors
    - MITRE's Common Weakness Enumeration (CWE)
    - False positives and false negatives

- Targeted static analysis
  - Proving targeted assertions
  - Counter examples
  - Program slicing

General Static Source Code Analysis

- Flagging programming errors
  - MITRE's Common Weakness Enumeration (CWE)
  - Security CWE's
    - Open Web Application Security Project (OWASP) Top 10 CWE's
      - Injection / Broken Authentication / Cross-site Scripting / Insecure Direct Object References / Security Misconfiguration / etc.
  - Safety CWE's
    - Data corruption CWE's
      - Shared resource race condition / Buffer Overflow / Improper Validation of an Array Index / Pointer Issues / Incorrect Type Conversion / etc.

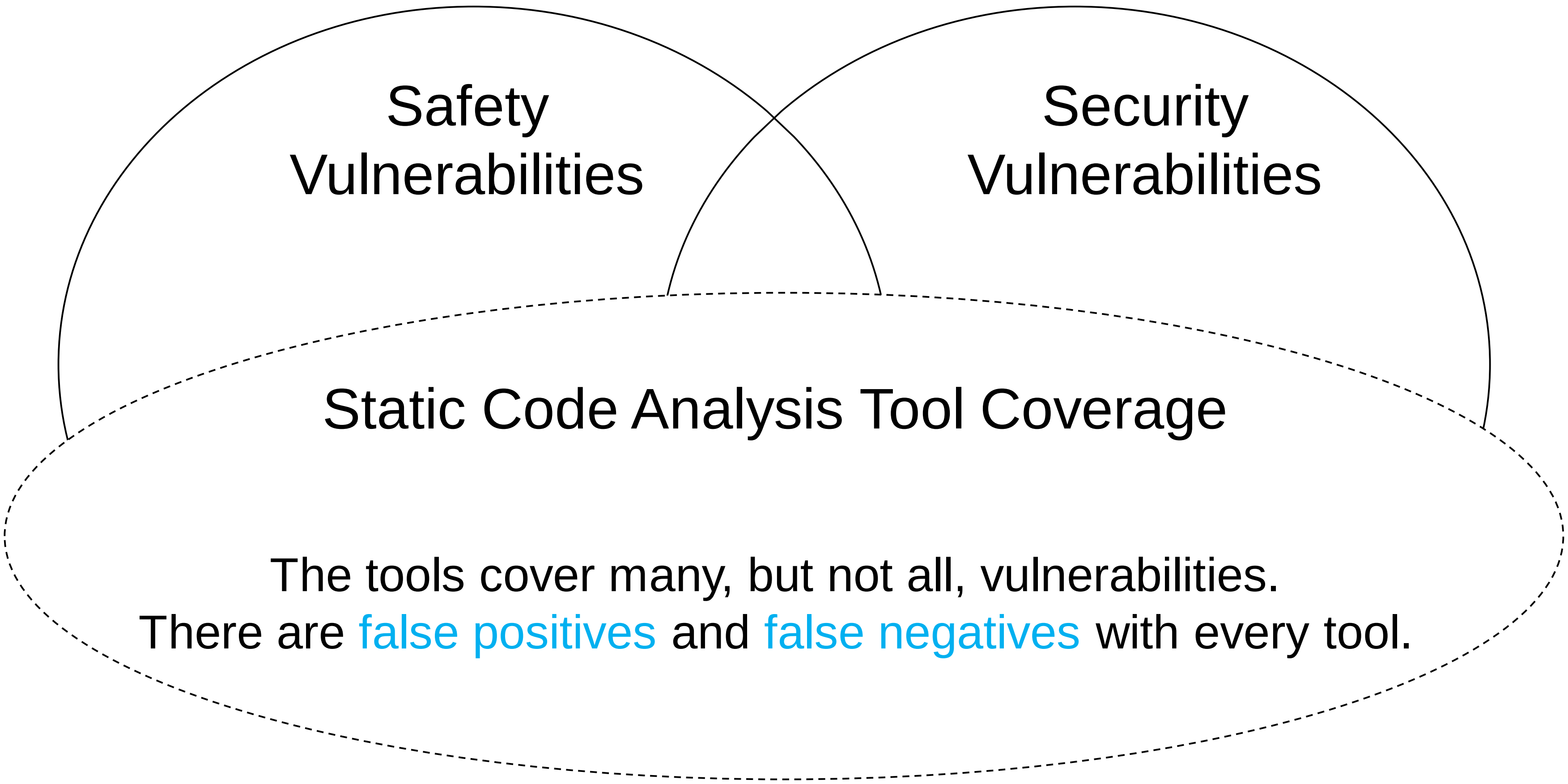
Safety Critical Data 'Corruption'

A correctly implemented algorithm operating on corrupted or stale safety-critical data can have unintended catastrophic results.

Some sources of corrupted data:

- Noise in digital message transmission
- Physical events/upsets during data storage
- Multi-threaded shared data
- Shared data between 'main' and Interrupt Service Routines
- Caching of data
- Loss of transient status data in failover or 'recovery'

General Static Code Analysis



The Opportunity for Software Safety

- Many of the programming errors detected by software static analysis tools used for cybersecurity have potential safety-critical impacts:
  - Multi-threaded race conditions
  - Mishandling of pointers
  - Incorrect casting (data type conversion)
  - Buffer overflow
- Providing access to general static analysis tools already being used for cybersecurity could greatly assist those responsible for software safety design and code analysis.
  - Need communication and coordination of effort between those responsible for security and those responsible for system safety

Static analysis tools are already in use for safety

- Food and Drug Administration (FDA):

  . . . static analysis examines the code exhaustively for certain kinds of insidious errors that are hard for human reviewers to detect.

  [http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm202511.htm#staticAnalysis]

- Federal Aviation Administration (FAA):

  A combination of both static and dynamic analyses should be specified by the applicant/developer and applied to the software.

  [Certification Authorities Software Team (CAST) Position Paper CAST-9, January 2002]

- Motor Industry Software Reliability Association (MISRA):

  Compliance with MISRA C/C++ coding standards for safety-critical software is checked by many static analysis tools.

Some General Static Source Code Analysis Tools

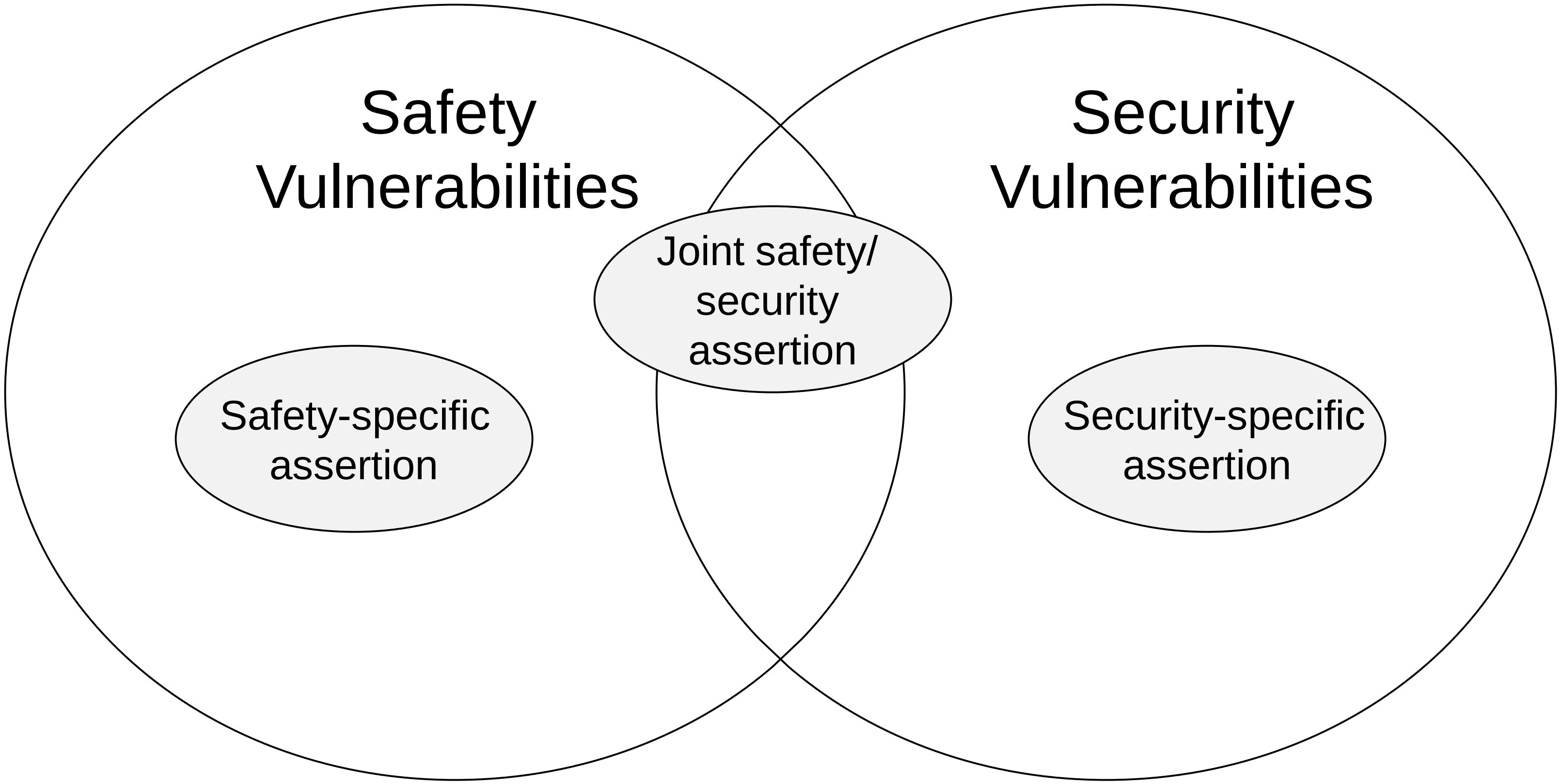
- Flagging programming errors
  - Grammatech's CodeSonar
  - Coverity's Code Advisor
  - IBM's AppScan
  - Clang Static Analyzer
  - CppCheck
  - Parasoft's Static Analysis Engine
  - Redlizard's Goanna
  - Checkmarx's CxSAST
  - Fasoo's Sparrow

Targeted Static Analysis:
Proving *specific properties* and *assertions*

Targeted Static Analysis

- Targeted static analysis
  - Proving targeted assertions
  - Counter examples
  - Program slicing

Targeted Static Analysis
Abstract Interpretation/Model Checking



"Prove" application-specific assertions hold true for any possible execution sequence (absence of *specific* vulnerabilities).

Soundness vs. Completeness

"[T]he essence of [abstract] static analysis is to efficiently compute approximate but sound guarantees: guarantees that are not misleading. . . . Due to the undecidability of static analysis problems, devising a procedure that does not produce spurious warnings and does not miss bugs is not possible."

["A Survey of Automated Techniques for Formal Software Verification" D'Silva, et al. IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. 27, NO. 7, JULY 2008]

Soundness means that, if the tool reports a property or assertion is met, the tool can be trusted.

Undecidability means that the tool might not be able to decide for every possible property or assertion (it is "incomplete").

Programming constraints to enable sound static analysis

- Specialized programing or modeling languages
  - Esterel/Lustre
  - Signal
  - Promela (for formal analysis by SPIN)
- Language subsets
  - Escher C Verifier (verifies programs written in an annotated C subset)
  - KeY (verifies properties of programs written in a Java subset)
  - VeriFast (verifies programs written in Java or C subsets)

Safety-Critical Decision Points

- Safety-critical software has command authority over potentially dangerous system actions.
- The software is therefore responsible for making the decision to take that action.
- If the data used to make the decision is corrupted or stale, the software can make the wrong decision with catastrophic results.
- Design and code analysis of the software should be focused on the integrity of the data used at each Safety-Critical Decision Point in the software.

Programming slicing

In computer programming, program slicing is the computation of the set of programs statements, the program slice, that may affect the values at some point of interest, referred to as a slicing criterion. Program slicing can be used in debugging to locate source of errors more easily. Other applications of slicing include software maintenance, optimization, program analysis, and information flow control.

[*Wikipedia* article on "Program Slicing," March 17, 2015]

Some Targeted Static Analysis Tools

- Proving targeted assertions (model checking)
  - Bell Lab's SPIN
  - Carnegie Mellon's NuSMV
  - Kestrel's CodeHawk (abstract interpretation)
  - MathWork's Polyspace Code Prover (abstract interpretation)
  - Microsoft-Inria TLA+ Proof System (TLAPS)
- Program slicing tools
  - VALSOFT/Joana
  - GrammaTech's CodeSurfer

Opportunities for software security/safety collaboration

[A]ll systems should be developed as safe secure systems. . . to allow for a complementary software skill set in software development (tools and language dependent). This would require a common development process rather than a skill change. . . [R]isk and hazard analysis, for both a security and safety assessment, should be conducted and therefore requires skills from both arenas . . . Independence of this skill . . . may be required though to ensure there is no bias towards contradicting risks.

[“Safety-Critical Versus Security-Critical Software.” Dr. Adele-Louise Carter, Version 1.0, August 2010, bcs.org.uk]

Questions?

Stuart Whitford
Senior Lead Scientist

Booz | Allen | Hamilton

Booz Allen Hamilton
1550 Crystal Dr, Suite 1100
Arlington, VA 22202
Tel (540) 903-7035
whitford_stuart@bah.com

Backup Slides

Tools to Support Software Safety Analysis

Use tools to help analyze the Safety-Significant Software in the context of the Architecture, Design, or Code (leverage those in use by the software developers or obtain):

- Software architecture and design modeling and analysis tools, such as those supporting Architecture Analysis and Design Language (AADL), Unified Model Language (UML), or Systems Modeling Language (SysML)
- Static code analysis tools that support focused design and code analyses, such as thread race/deadlock detection or program slicing
- Source code cross reference tools that support searching, cross-referencing, and navigating (forward and backward) source code trees

Some References

- Joint Software Systems Safety Engineering Workgroup. (2010). Joint Software System Safety Engineering Handbook (JSSSEH). Indian Head, MD: Naval Ordnance Safety and Security Activity.
- Anton, J. et al (2005). “Towards the Industrial Scale Development of Custom Static Analyzers.”
- NSA Center for Assured Software (2011). “On Analyzing Static Analysis Tools.”
- NIST Special Publication 800-176 (2014). *Computer Security Division Annual Report 2014*.
- Garavel, H., ed. (2013). *Formal Methods for Safe and Secure Computer Systems*. BSI Study 875.
- Carter, A. (2010). *Safety-Critical Versus Security-Critical Software*.
- Moy, Y. (2014). “Static Analysis Tools Pass the Quals.” *CrossTalk*. November/December, 2014.

Implementation of Clustering Analysis in Engineered Resilient Systems Tools for Enhanced Trade Space Exploration of Military Ground Vehicles

Mr. Andy Pokoyoway*, Dr. Matt Castanier

US Army Tank Automotive Research, Development, and Engineering Center (TARDEC)

Abstract ID: 19712 *** Lead author contact info:** 586-282-3765 <andrew.p.pokoyoway.civ@mail.mil>

NDIA Systems Engineering Conference

Springfield, VA 26 OCT 2017

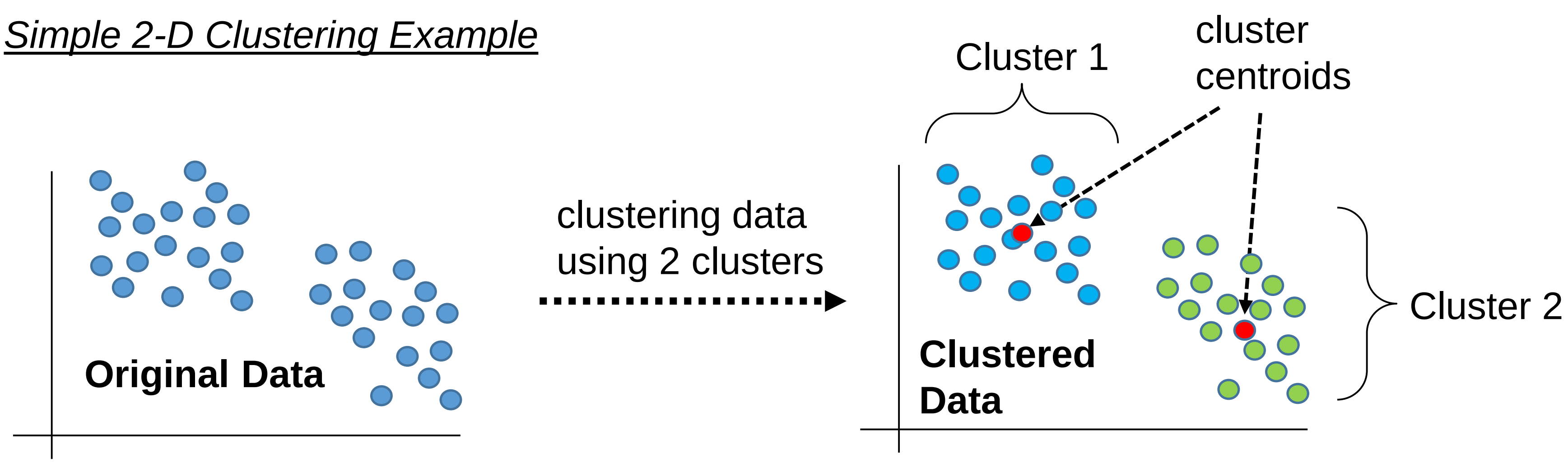
Background and Motivation

- Performing multidisciplinary design optimization of a military ground vehicle is extremely challenging
- One challenge is related to analyzing large, highly dimensional vehicle design datasets
- Analysis questions to answer regarding these datasets:
  - Do my highest-ranked designs reside in multiple regions of the trade space?
  - How many promising regions are there?
  - Does each region represent variations on a single design concept or multiple design concepts?
  - How can I best characterize the unique features of each design concept?

Clustering

- Simply put, clustering is the process of assigning data points to groups based on how closely their values are to a common group centroid
- A way to group data that is highly dimensional
- Different algorithms available
- Machine learning technique

Simple 2-D Clustering Example



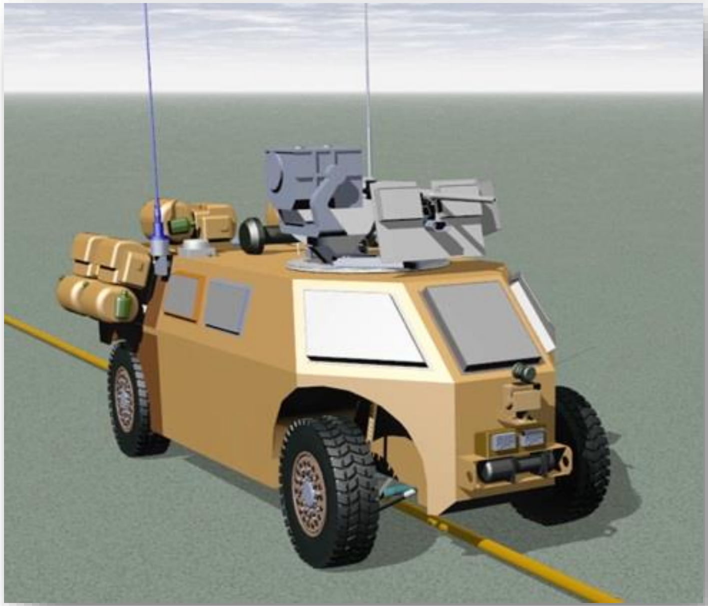
Clustering for Trade Space Design Populations

- Reduce large, highly dimensional datasets to more manageable, digestible sizes. This can make it easier to draw conclusions
- Automated way of quantifying and qualifying design differences - ***characterizing***; may help answer the question of : “How different are the top ranked vehicle designs?”
- Clusters could be used to provide promising vehicle design groups, and therefore promising characteristics, to be taken to the next stage of vehicle development

ERS LRV Trade Space Exploration Project

Objectives

- Learn, evaluate, and provide feedback to developers of **CREATE-GV and ERS Tools**
- Apply these tools to the **LRV notional concept vehicle** to perform **trade space exploration**
- Develop new trade space exploration methods for ground vehicles



CREATE-GV: Computational Research and Engineering Acquisition Tools and Environments – Ground Vehicles

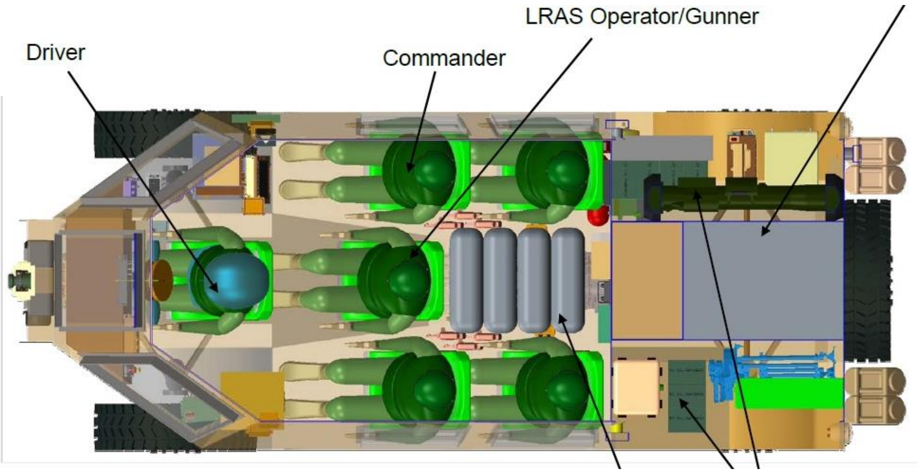
ERS: Engineered Resilient Systems

LRV: Light Reconnaissance Vehicle

LRV – A Notional Concept for a New-Start Vehicle

Notional concept was initially developed based on these requirements:

- Crew of 6
- Power for 96-hour mission
- Silent watch, silent move
- Advanced reconnaissance & surveillance equipment package
- CH-47 internal transport and sling-load transport



Trade Space Exploration Process

Reviewed initial concept
& requirements

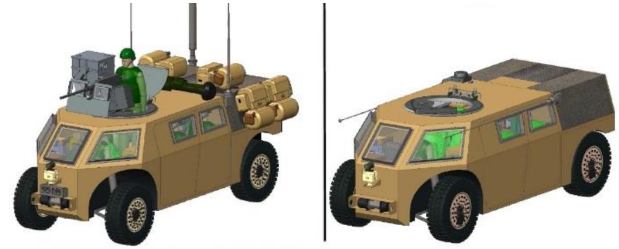
Performed analysis to
build trade space

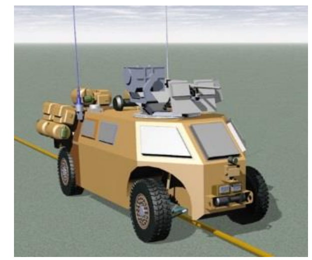
Revisited concept &
varied requirements

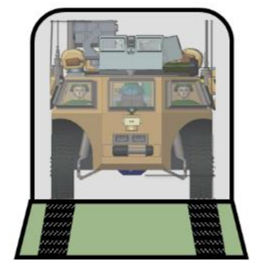
Performed analysis to
expand trade space

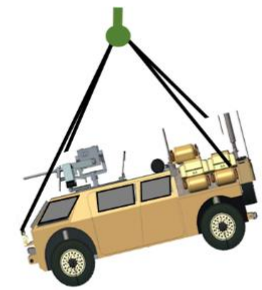
Generated new design
set = new concept

Iterative Concept-Analysis Loop









Trade Space Exploration Process

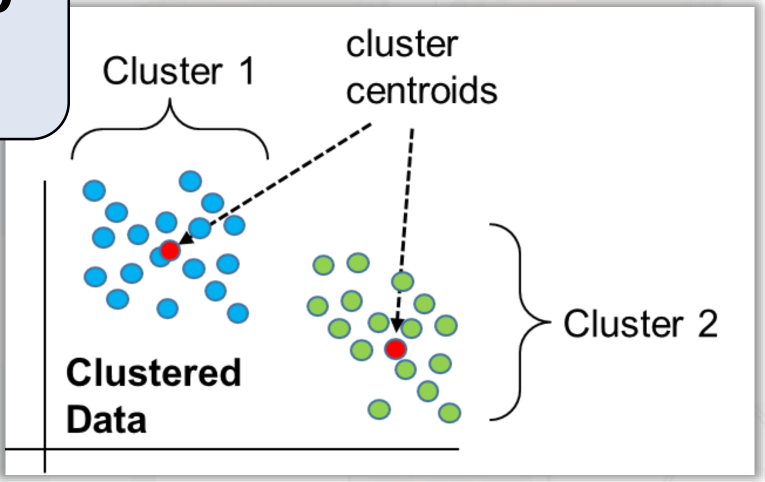
Reviewed initial concept & requirements

Performed analysis to build trade space

Revisited concept & varied requirements

Iterative Concept-Analysis Loop

Clustering Analysis



Performed analysis to expand trade space

Generated new design set = new concept

Trade Space Construction in ERS TradeBuilder

CREATE-GV

1. On-Road Speed
2. Off-Road Speed
3. Max Sandy Grade
4. Off-Road No-Go %
5. Soft-soil mobility

ERS TradeBuilder

1. Surveillance
2. Crew
3. Stability
4. Silhouette
5. Power density
6. Survivability
7. Transportability
8. Lethality

Performance Metrics imported from result files

Performance Metrics evaluated in ERS TradeBuilder

Design Variables

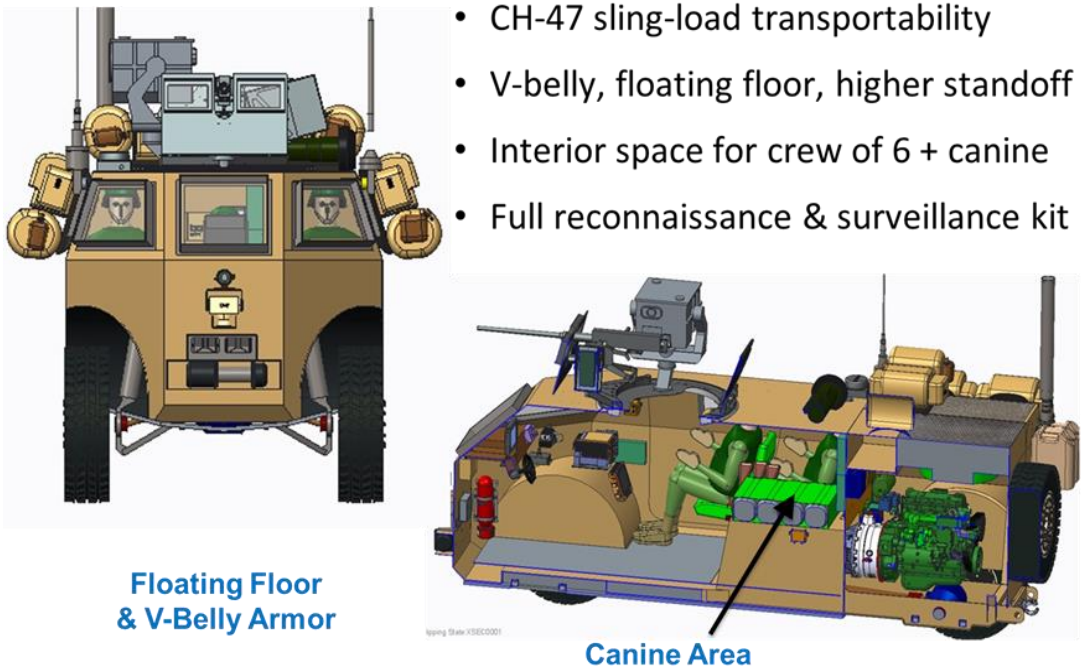
Designs

#	H	L	W	…													
1	H_1	L_1	W_1														
2	H_2	L_2	W_2														
3	H_3	L_3	W_3														
4	H_4	L_4	W_4														

⋮

Trade Space Vehicle Design Characterization

- Common features from highest-ranked designs:

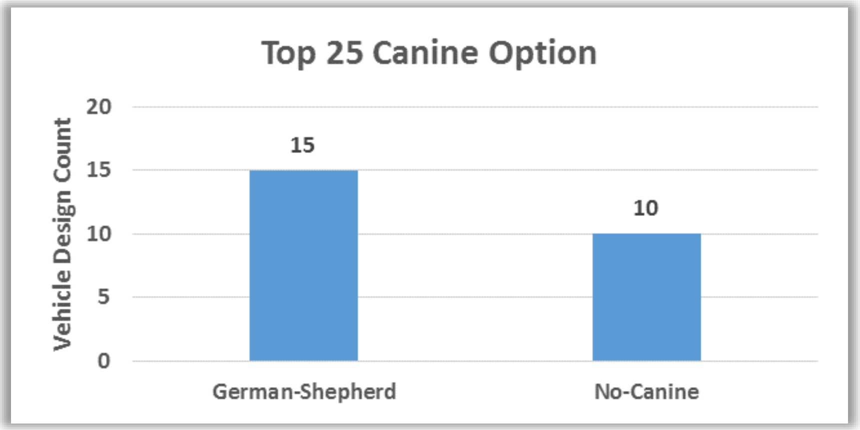


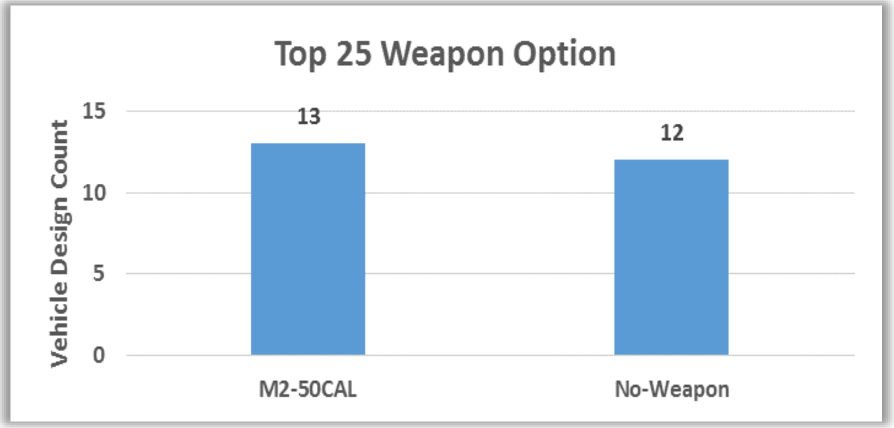
- CH-47 sling-load transportability
- V-belly, floating floor, higher standoff
- Interior space for crew of 6 + canine
- Full reconnaissance & surveillance kit

These are general features typically seen in the top 25 ranked vehicles, **though not all of the top 25 designs had the same features**

Trade Space Vehicle Design Characterization

- Two areas where differences are seen in the top 25 designs :



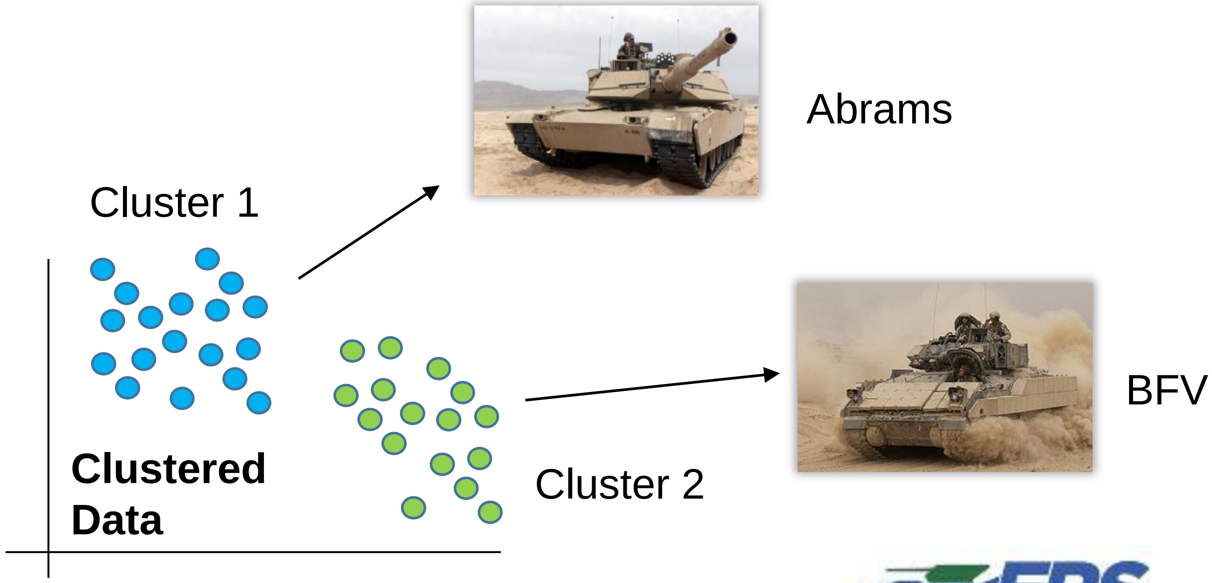


- Characterizing the top ranking designs as a whole may not lead to as useful conclusions regarding which features a <u>single</u> vehicle design should have
- We could be **unintentionally characterizing multiple vehicle designs, multiple variants**, *a potential outcome when performing multi-objective design optimization*

Trade Space Vehicle Design Characterization

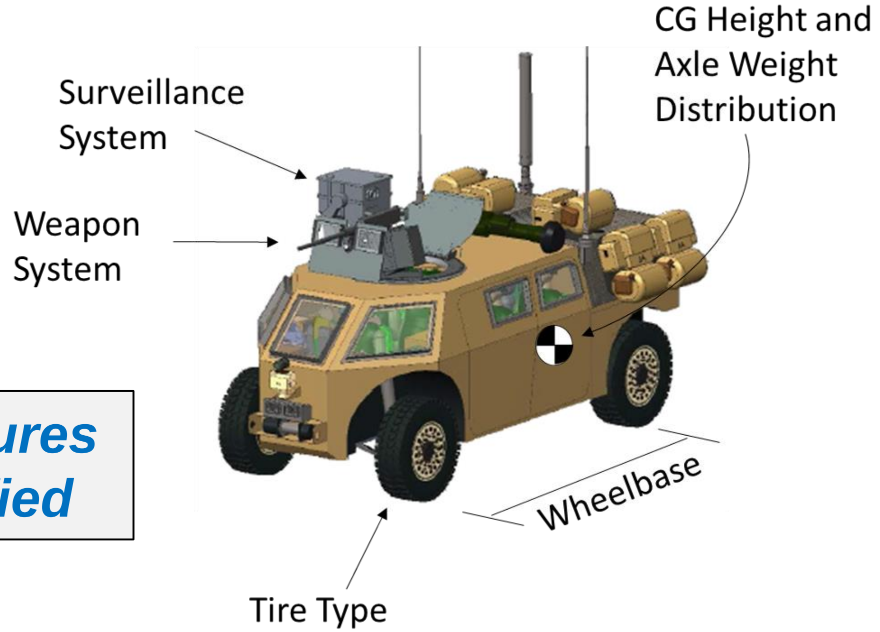
- Early in the concept development phase, the trade space is large, with a design space that could be spanning regions consisting of two or more completely different vehicle designs
- … and this is not apparent
- We want to understand if potential regions exist early on in the analysis process to understand what unique concepts we may have

Potential example outcome of early concept, highly dimensional, multi-object design optimization



Clustering Analysis - Setup

- **K-means clustering** algorithm used within R ("Hartigan-Wong" version)
- **Chose to generate 10 clusters** based on the "within sum of squares (WSS)" count selection method
- Design variables and characteristics chosen for features:



- Suspension characteristics (damping ratio and ride frequency) for the front and rear axles
- Canine
- Crew size
- Armor weight

13 features specified

Clustering Analysis - Setup

Design Variables | *CREATE-GV Performance Metrics* | *ERS TradeBuilder Performance Metrics*

Designs

#	H	L	W	...
1	H_1	L_1	W_1	
2	H_2	L_2	W_2	
3	H_3	L_3	W_3	
4	H_4	L_4	W_4	

⋮

976 designs

Matrix representation of the trade space

Assigned Cluster added

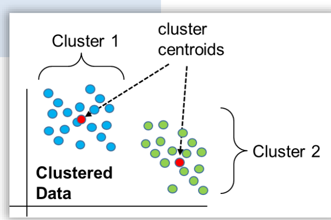
13 selected features

Designs

#	F1	F2	F3	...
1	H_1	L_1	W_1	
2	H_2	L_2	W_2	
3	H_3	L_3	W_3	
4	H_4	L_4	W_4	

⋮

Clustering Analysis using R



13 selected features

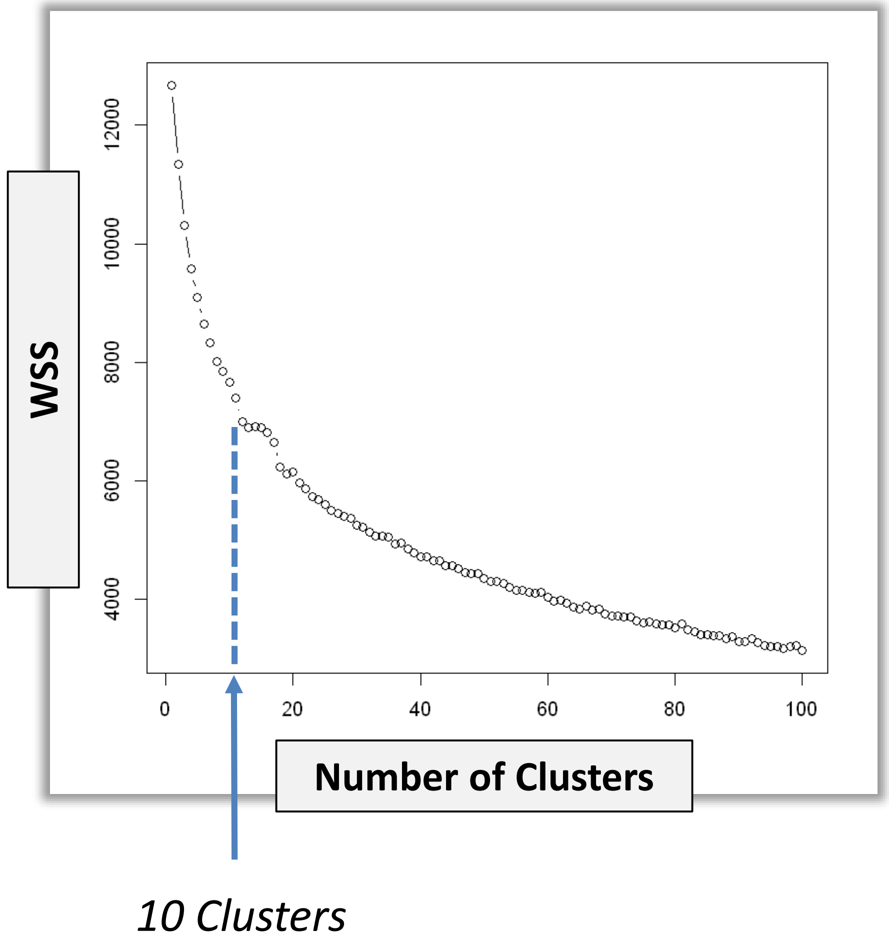
Designs

#	F1	F2	F3	...	C#
1	H_1	L_1	W_1		1
2	H_2	L_2	W_2		7
3	H_3	L_3	W_3		4
4	H_4	L_4	W_4		3

⋮

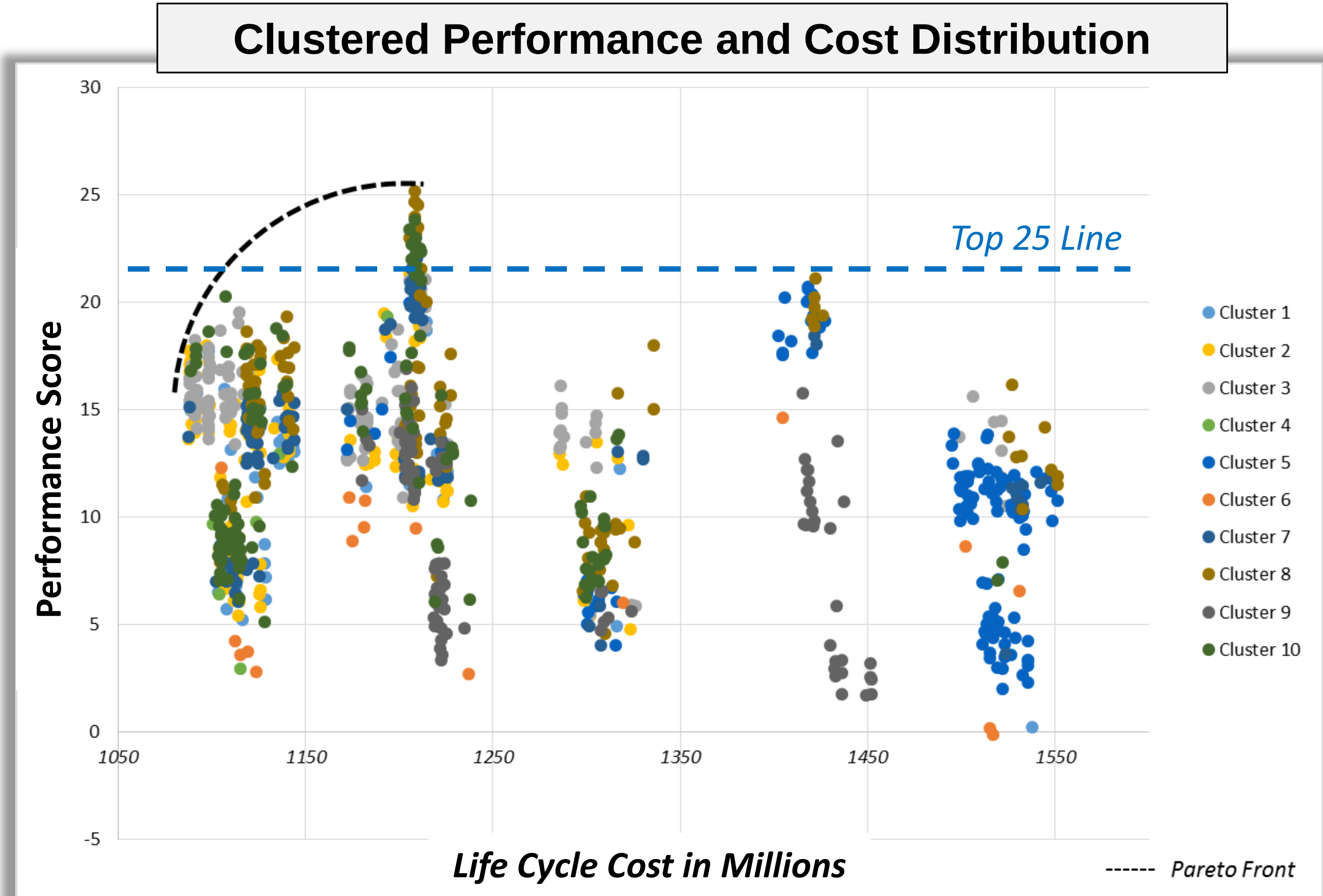
Clustering Analysis – Selecting Cluster Count

- Within Sum of Squares cluster count selection method (WSS)

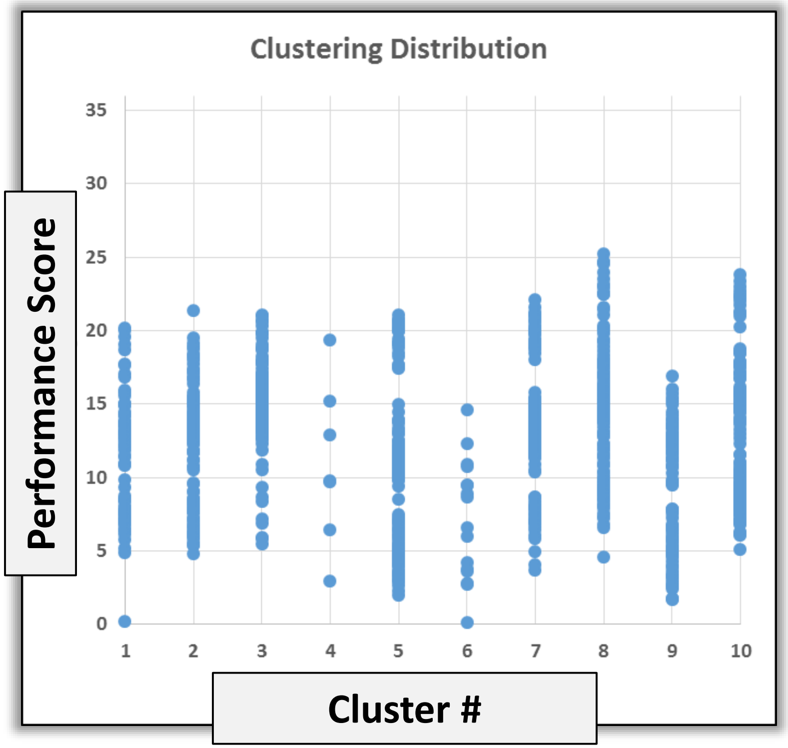


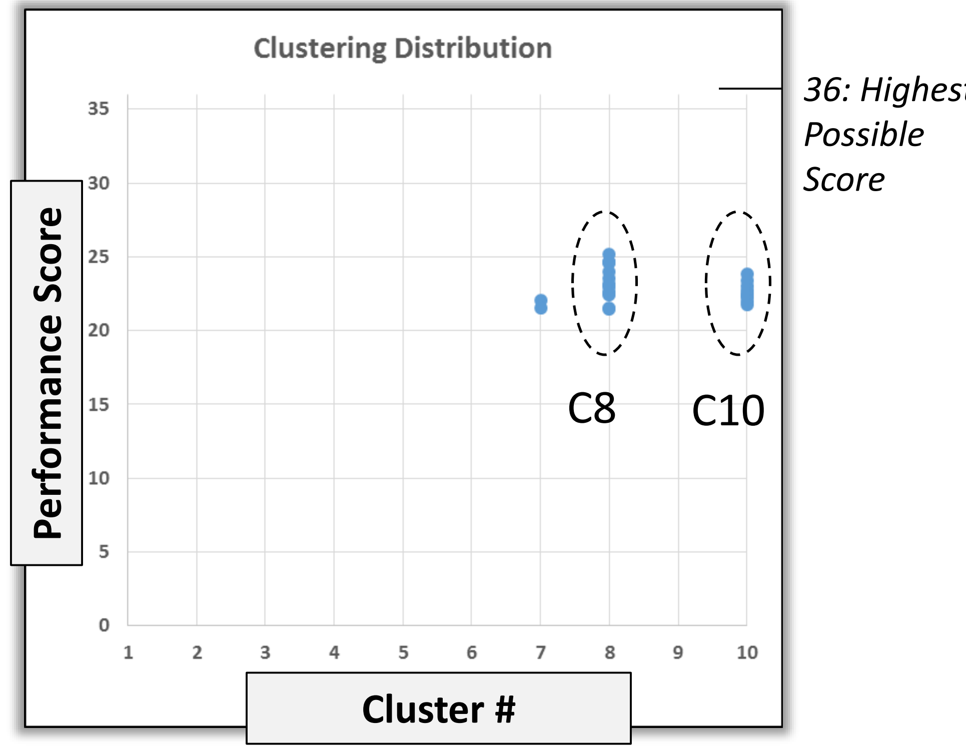
… at 976 clusters, the sum of squares value would equal 0

Clustering Analysis – Results



Clustering Analysis – Characterization





Plot shows clustering results using 10 specified clusters for the 976 vehicles designs investigated

Showing 3 clusters in the top 25:

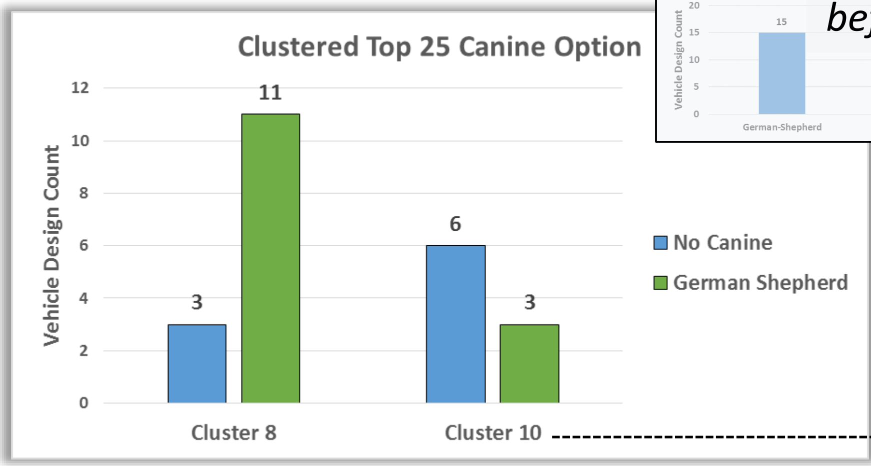
Cluster 7 (C7) : 2 designs

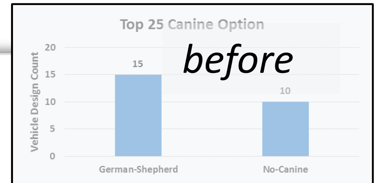
Cluster 8 (C8) : 14 designs

Cluster 10 (C10) : 9 designs

Clustering Characterization Comparison

- *Looking at the same two features as before…*



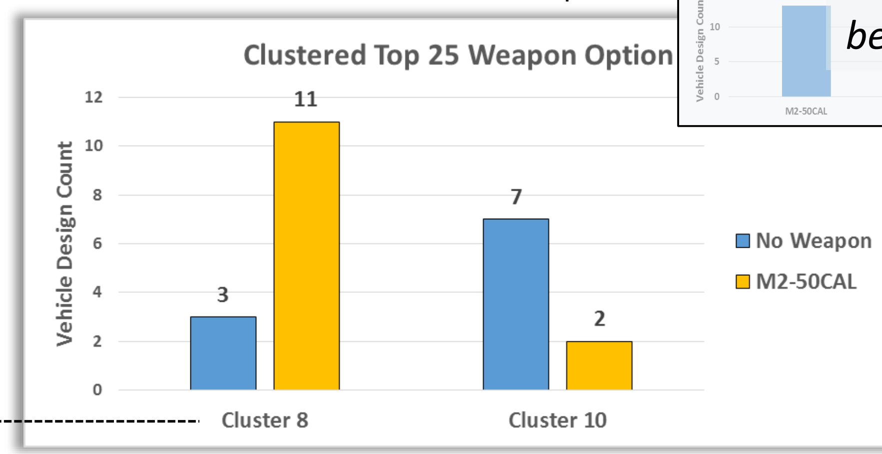


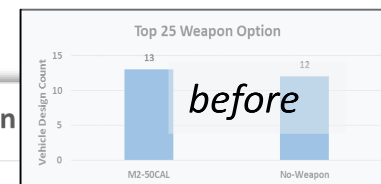
Cluster 10 Designs:

Mostly <u>do not</u> include a weapon or canine

Cluster 8 Designs:

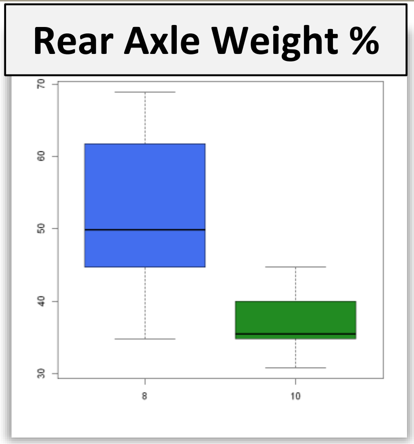
Mostly include weapon and canine

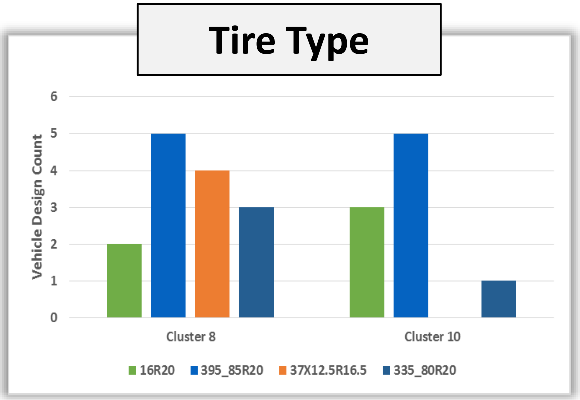


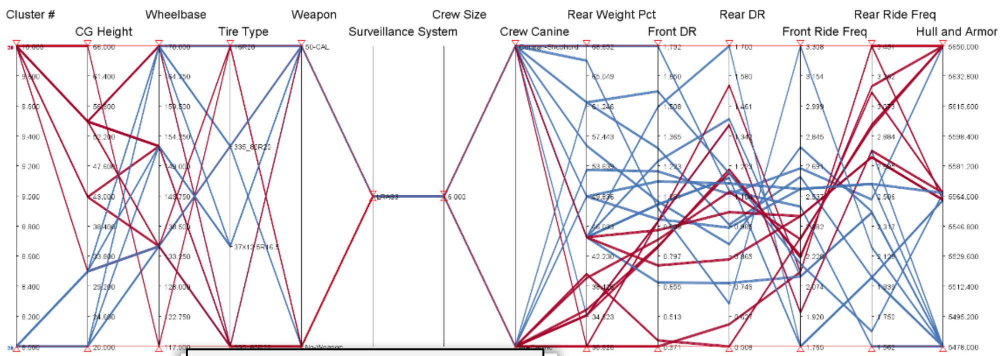


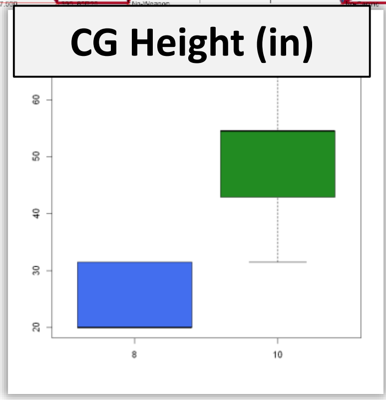
Clustering Characterization - Features

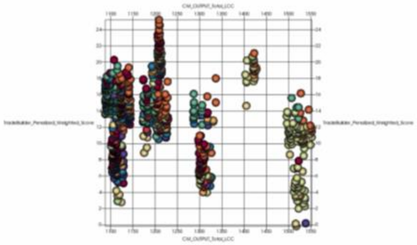
- Various visualizations used to distinguish the differences between the top 25 designs within **clusters 8** and **10** concerning their *design variables and characteristics*











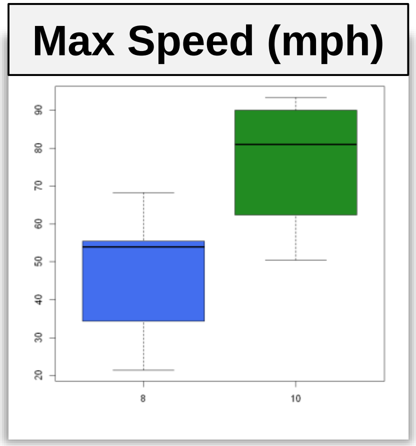
Clustering Characterization - Features

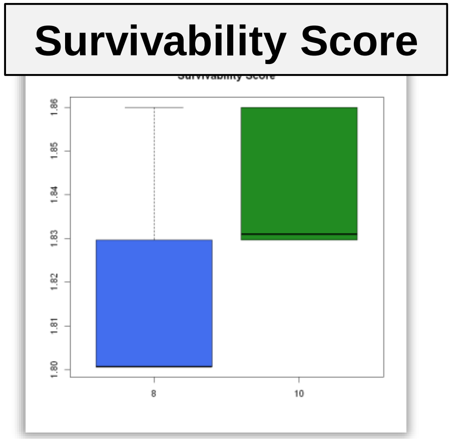
Feature	Cluster 8	Cluster 10
Weapon	Most designs include the M2-50 Cal	Most designs don't include a weapon
Canine	Most designs include a German Shepherd	Most designs don't include a canine
CG Height	Low	High
Wheelbase Length	Longer	Medium
Weight Distribution	More centered to rear heavy designs	More front heavy designs
Front Axle Ride Characteristics	Stiff, Mostly Overdamped	Less Stiff, Underdamped
Rear Axle Ride Characteristics	Stiff, Mostly Overdamped	Very Stiff, Mostly Overdamped

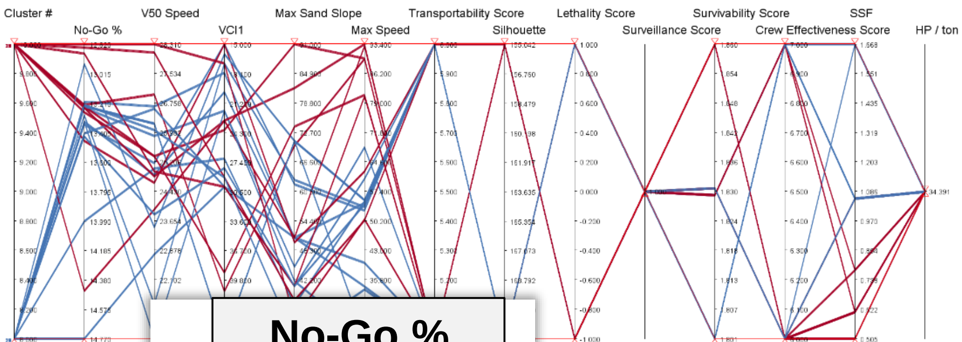
These clustered designs were **similar regarding the Tires, Hull and Armor Weight, Crew Size, and Surveillance System** features

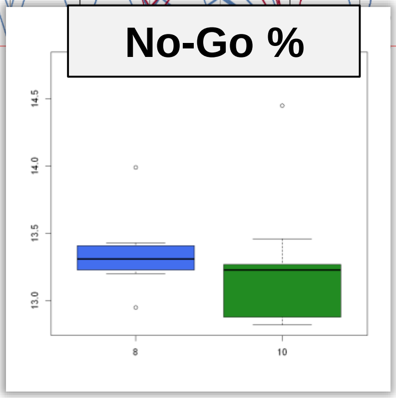
Clustering Characterization - Performance

- Various visualizations used to distinguish the differences between the top 25 designs within **clusters 8** and **10** concerning their *performance*









Clustering Characterization - Performance

Performance	Cluster 8	Cluster 10
Crew Effectiveness	Highest score	Meets requirements
Max Speed	Lower to moderate	Moderate to high
Max Sand Slope	Medium	Medium to high
SSF	High	Medium to low
Visibility (Silhouette)	Larger profile	Smaller profile
Lethality	Higher	Lower

These clustered designs were **similar regarding the Surveillance, No-Go %, VCI1, V50 Speed, HP / ton, Survivability, and Transportability** performance metrics

Clustered Characterization - Conclusions

- Highlighted two main clusters in the top 25 ranked vehicle designs and analyzed their features and performance
- Instead of describing one LRV design, now describing two LRV design variations in the top 25 – two designs that have some distinct differences, but with similar overall performance scores

Cluster 8

Well-rounded design concerning all of the areas of performance considered

Two potential variants

Cluster 10

Fast, mobile design, with smaller profile

Conclusions

New trade space exploration process *which utilized a* ***clustering technique*** *highlighted* ***two main vehicle variants*** *out of a set of top performing vehicle designs*

- Clustering is a promising trade space analysis process addition to help improve and further automate trade space characterization
- Can help answer important questions about a trade space
- And lead to improved optimal design extraction from trade spaces, and overall improved concept design development
- More to look into : clustering technique tuning and feature selection

Acknowledgments: ERS, CREATE-GV, ECO

US Army TARDEC

- Stuart Parkhurst
- Jacob Woten
- Stephanie Loewen
- Joe Raymond
- Scott Shurin
- Ian Stranaly
- Tom Skorupa
- Gary Bronstetter
- MAJ Roy
- COL Vanyo
- …

US Army ERDC

- Alex Baylot
- Owen Eslinger
- Justin Foster
- Willie Brown
- Daniel Chaussé
- Jody Priddy
- Chris Goodin
- Jessica Johnson
- Glover George
- Timothy Garton
- …

Thank you!

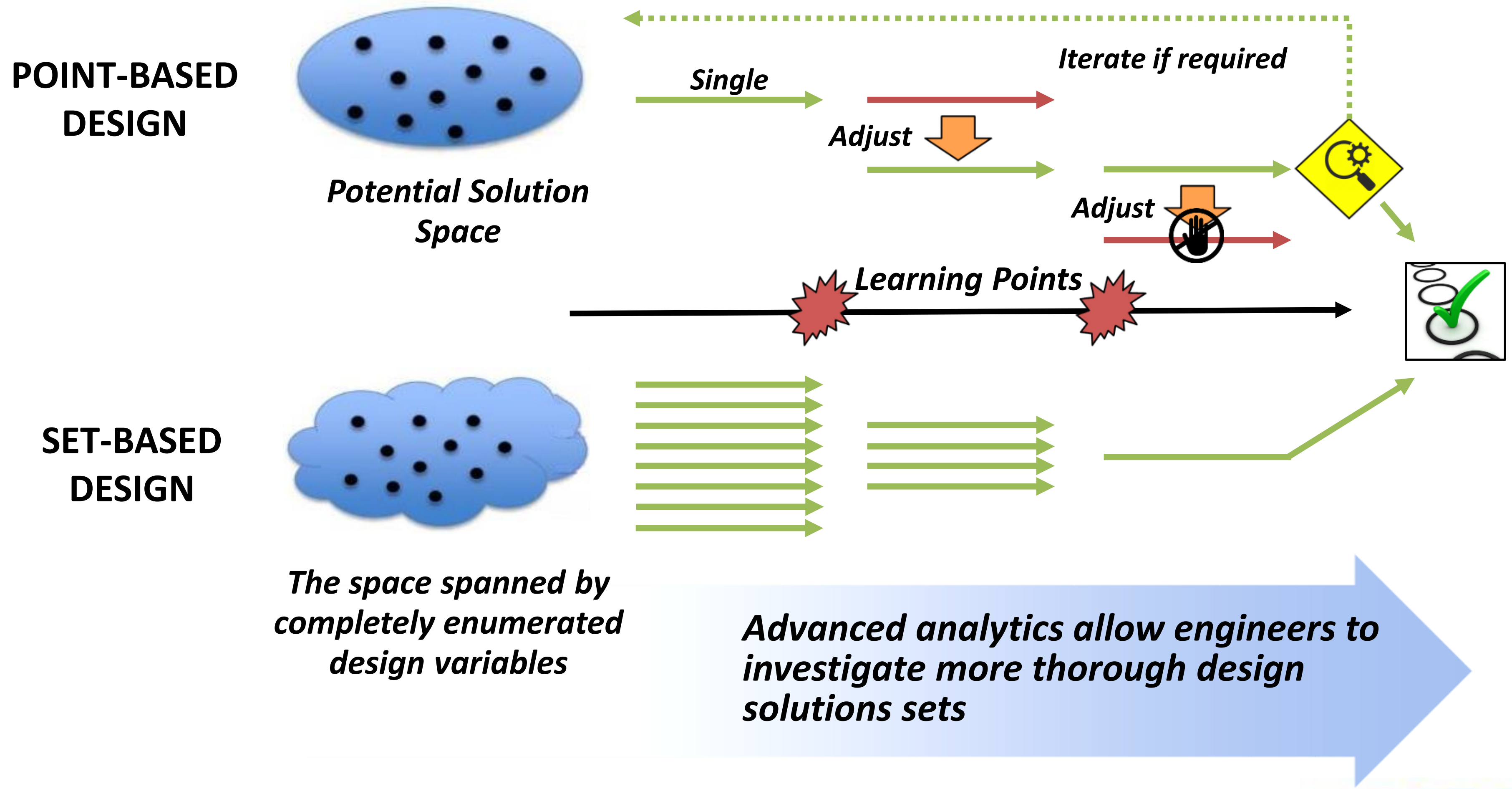
Tradespace: Informed Decision-making for Acquisition

20th Annual NDIA Systems Engineering Conference
October 26, 2017

Timothy Garton
Computer Scientist
US Army Corps of Engineers
Engineer Research Development Center

Tradespace Analytics - Set-Based Design

Tradespace - the set of processes, program and system parameters, attributes, and characteristics required to satisfy mission profile



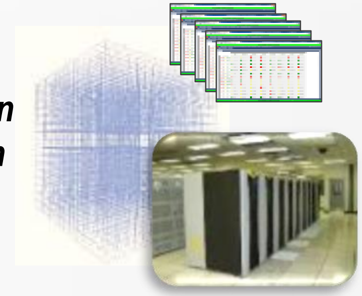
ERS Tradespace Concept

- *Architecture*
- *Tradespace Analytics*
- *Advanced Modeling*
- *Environmental Rep.*
- *Mission Context*

Cost models
-ilities
….other

ERS CLOUD COMPUTING ENVIRONMENT (CCE)

10,000x
Improvement in productivity in Analysis of Alternatives



Efficiently discover key performance parameters (KPPs)

HPCMP and S&T Resources

Currently Applied ERS Advanced Tradespace Analytics

DEFINE

- Early concept tool
- Functional / component breakdown
- Explore tradespace edges

Expand Tradespace Fully

Performance Assessments
Performance Metrics

High-fidelity Models
Parameter Sweeps:
Design Variations

ANALYZE

- Highly computational
- Sifts through millions of designs
- Refined set of specifications for viable design solutions

Tradespace Exploration Processes

physics-based models analyze new designs

known designs are used in formulating the tradespace

Seeding

High-Fidelity Simulations

Historical Data

evaluated in various performance scenarios

Performance Modeling

analyzed from a systems perspective

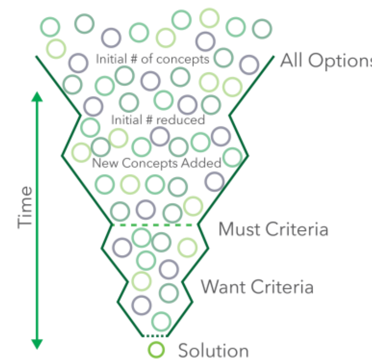
Systems Properties "ilities"

assessed in the context of possible operational missions

Mission Modeling

Tradespace Creation *"Define"*

Tradespace Analysis *"Partition"*



Exclusion

Tradespace is gradually narrowed

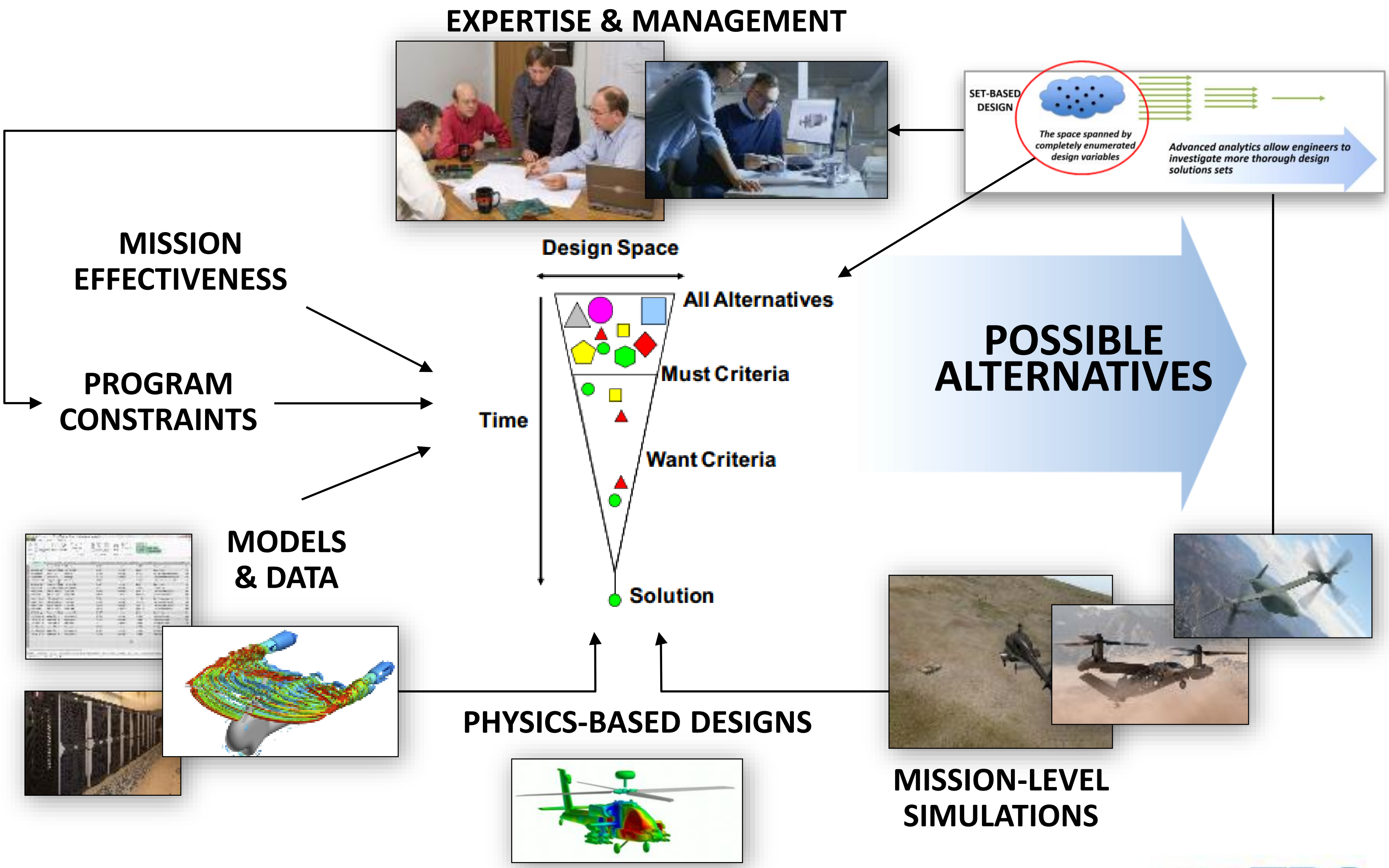
Selection

Globally optimum solutions are revealed

Comparison

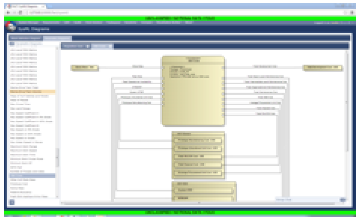
Remaining designs are compared and contrasted

Decision Analysis: Integrated Processes with Trade Analytics

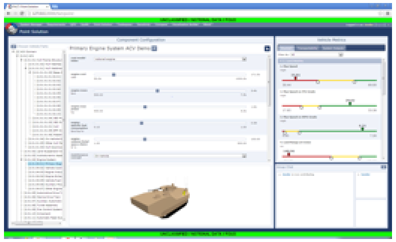


Technical Requirements of Data-Driven Decisions Tools

Trace Requirements and link systems to output

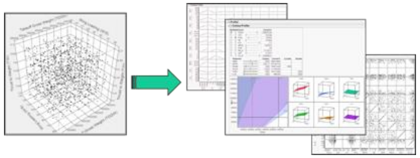


Visualize trades between dominant variables and requirements



Allow novice and advanced data exploration

Quickly find dominant variables



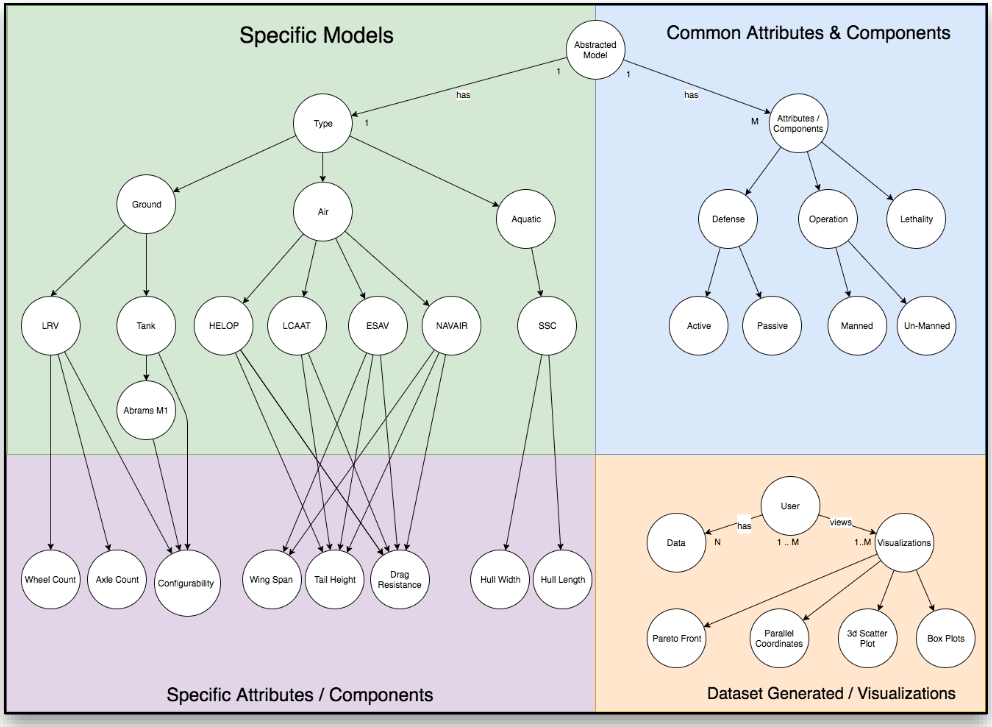
Tradespace tools must:

- Have a traceable history
- Utilize cutting edge search and decision analytics

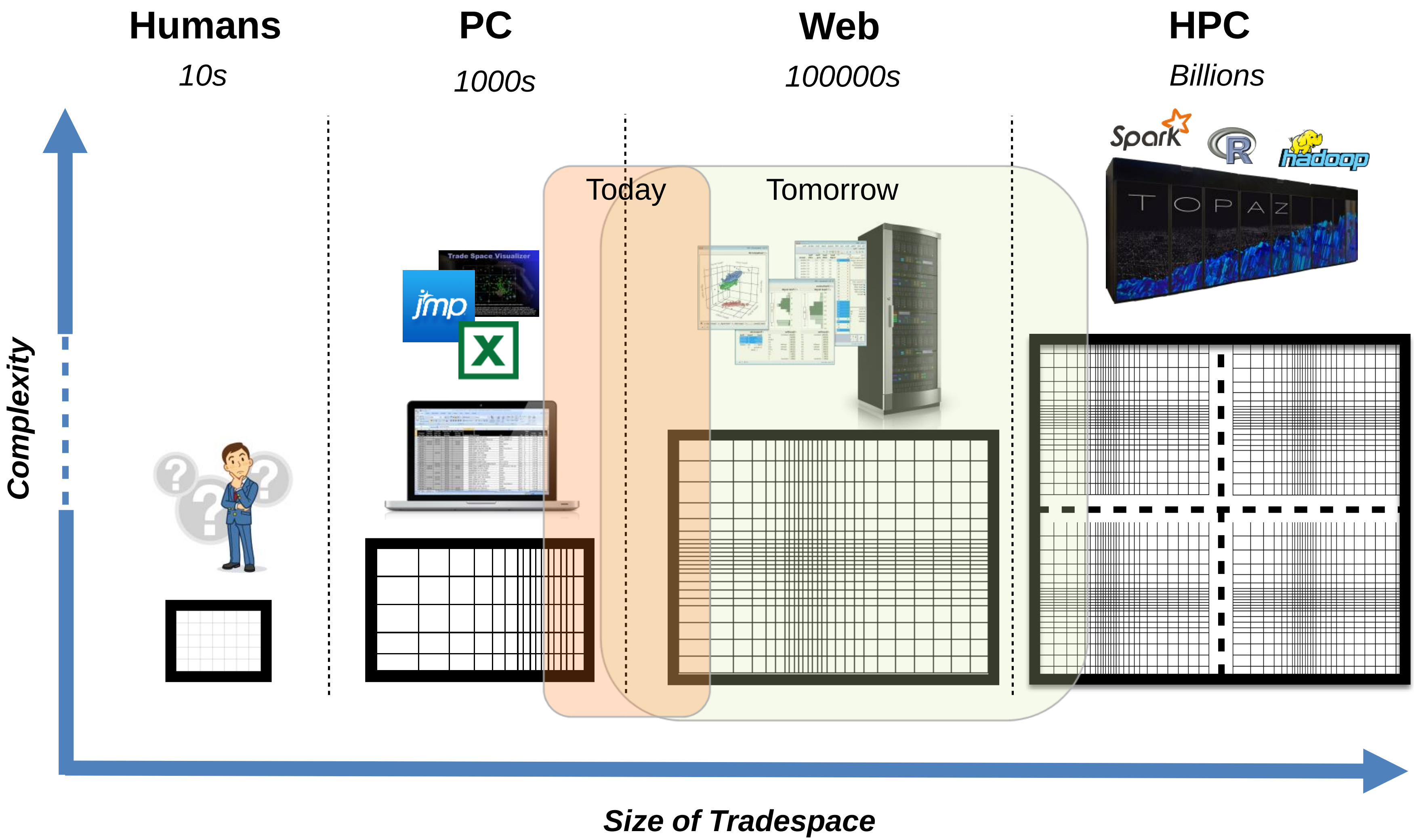
Ontology Models: Consistency in System Communication

Original system breakdowns by ontologies or SysML, along with requirements, are tied to the tradespace

- **Inserts greater accuracy and verification into the analytic processes**
- **Passing the metadata gives us insight into how to analyze the data**
- ***Direct mapping via SysML → WBS → MILSTD-881C (soon 881D) is an OSD-CAPE requirement***



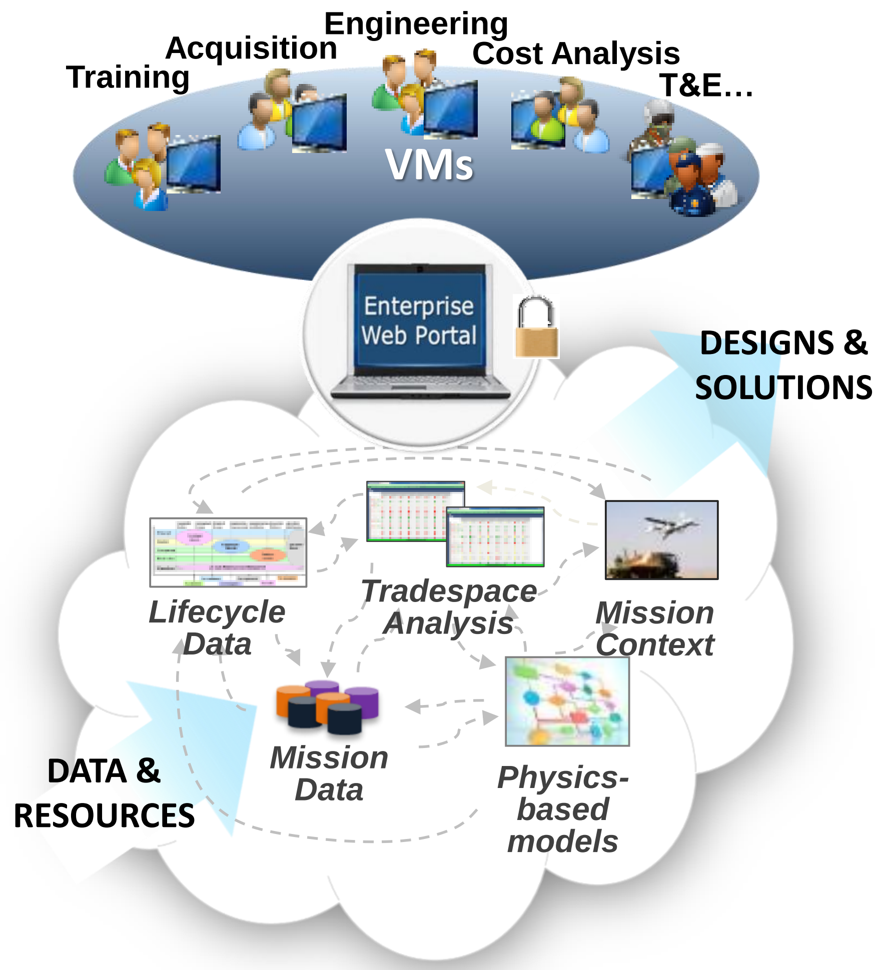
Data Metrics



Tradespace Analytics – Data Analysis and Visualization Tool

Beta-Release Status:

- **Supplied acquisition community a web-based environment for storing, visualizing and analyzing data**
- **Allowed for access and annotation by multiple parties for any given location;**
- **Provided the base for a collaborative decision support environment.**
  - Gaps in previous environments forced point-based design methodology.
- **Successfully supported MBSE and data filtering**
  - Previously available MBSE were expensive and resource heavy – requiring local resources and administrative personnel, required expensive licensing agreements.



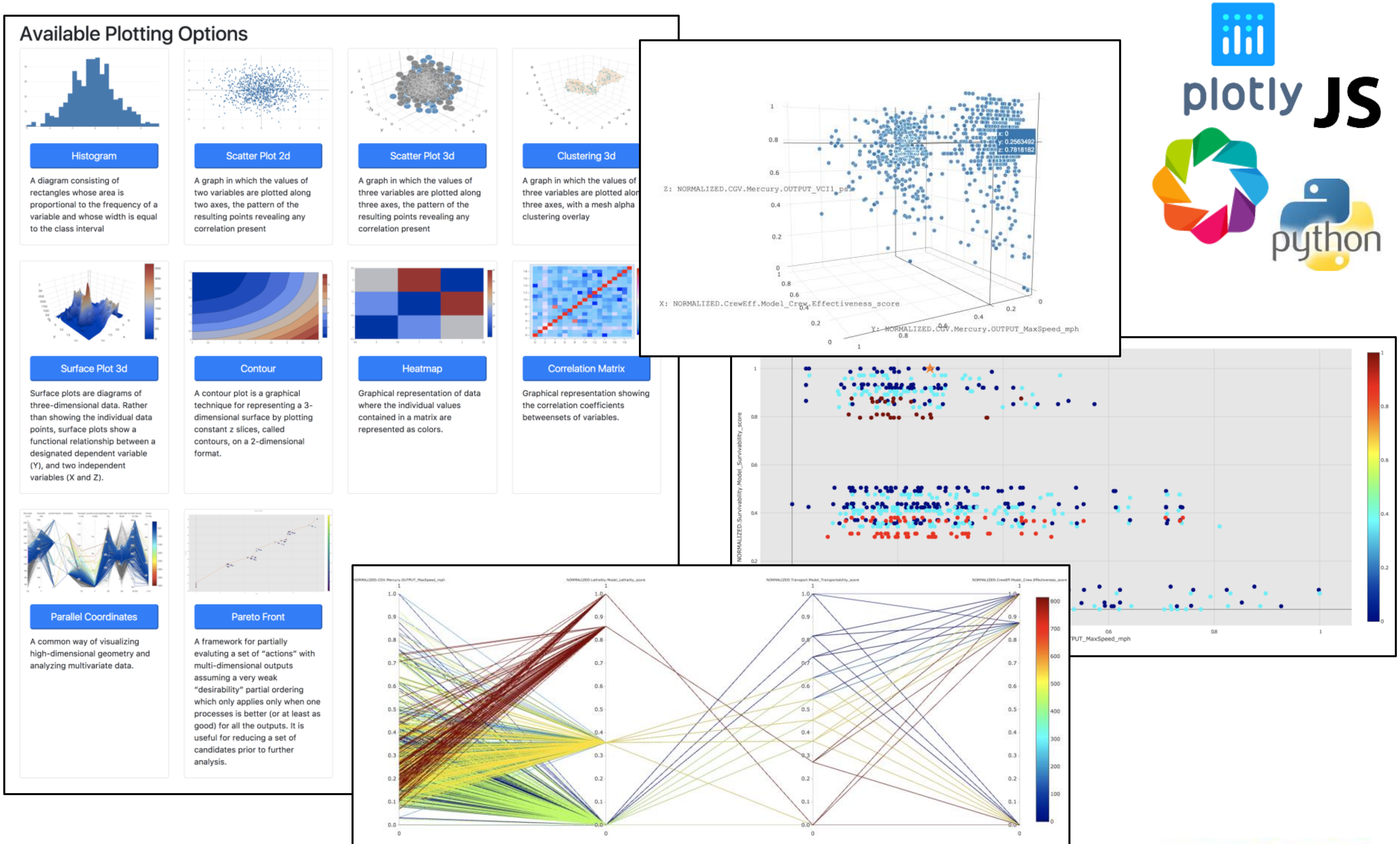
Tradespace Analytics Beta Release Lessons Learned

The FY17 Beta Release of TradeAnalyzer to a number of DoD Users resulted in important lessons and changes

- **Use of ParaView Web - generating interactive visualizations of large data-sets and annotation capabilities**
- **Role Based Access Control (RBAC) needed to execute R-Scripts in a secured environment; implementation in a complex collaborative environment is challenging.**
- **Working on secure authentication mechanisms that couple with customers local access control policies is an ongoing and important DoD issue.**

ERS Tradespace development is now focusing on the user-oriented approach in preparation for DoD-wide implementation and adoption

Tradespace Analytics and Visualizations



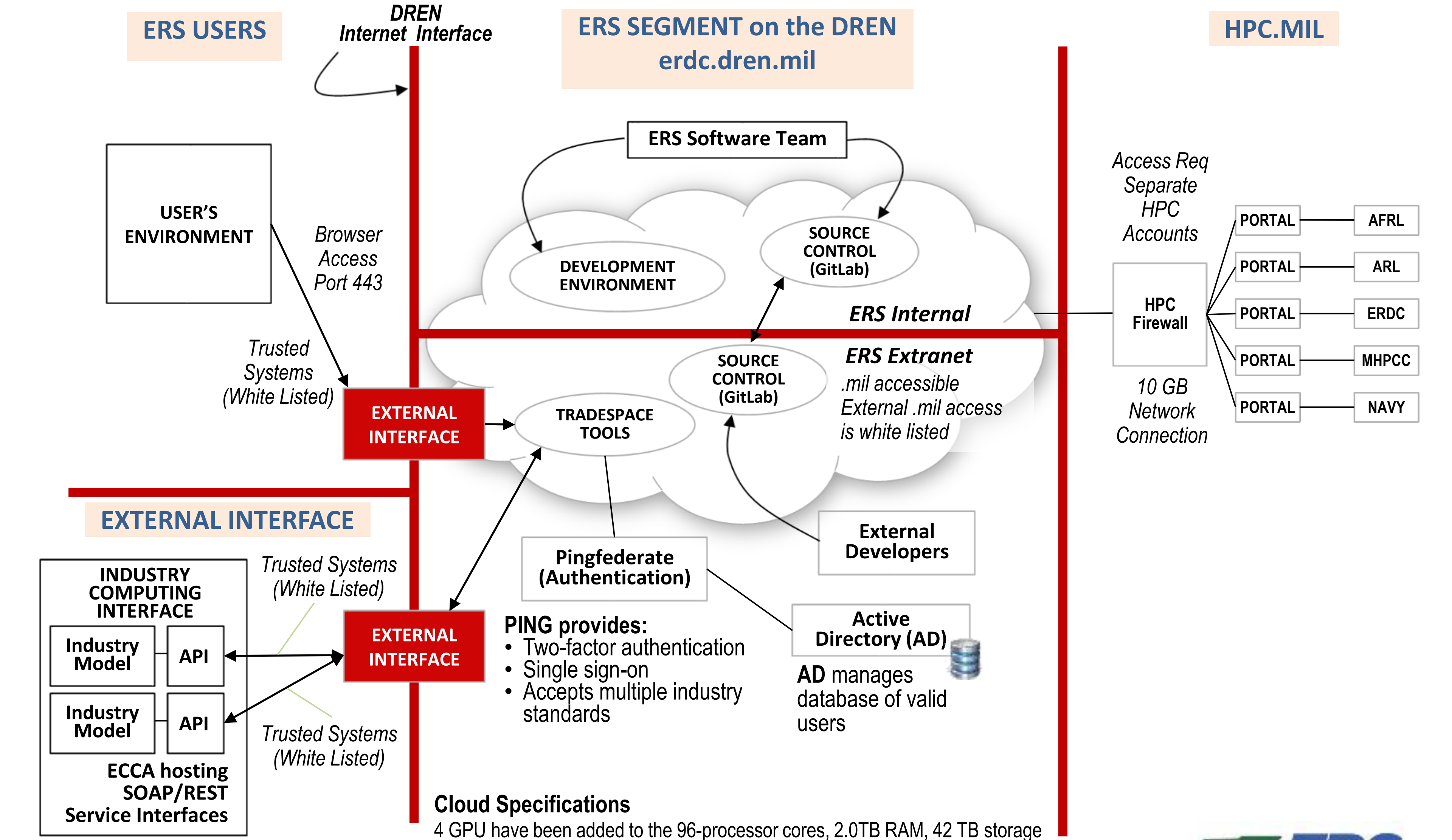
Updates to Architecture

- ***Web Hosted***
- ***Access Control***
- ***Collaboration***
  - ***Shared Notebooks***
  - ***Shared Data***
- ***Versioning***
- ***Analytic Packages***
- ***Scalable***
- ***Portable***
- ***Reproducible***
- ***Distributed***
  - ***Spark***
  - ***Hadoop***

Relevant ERS NDIA Talk

10:40 - Resilient Tools: Building an Agile Framework for the Analysis of Environmental Impacts on Military Systems
Dharhas Pothina, PhD - ERDC

Network Access



Questions

ERS NDIA
FUELING INNOVATION & COLLABORATION

Backup Slides

What is a Tradespace

- **Tradespace is the space spanned by completely enumerated design variables. It is the potential solution space.**
- **Tradespace can also be defined as the set of processes, program and system parameters, attributes, and characteristics required to satisfy mission profile.**
- **The enumeration of a large tradespace helps prevent designers from starting with point designs while allowing them to investigate more thorough design solutions sets.**

System-Supported Collaboration Supports Data-Driven Decision-Making

ERS Tradespace Analytics support Collaborative Processes

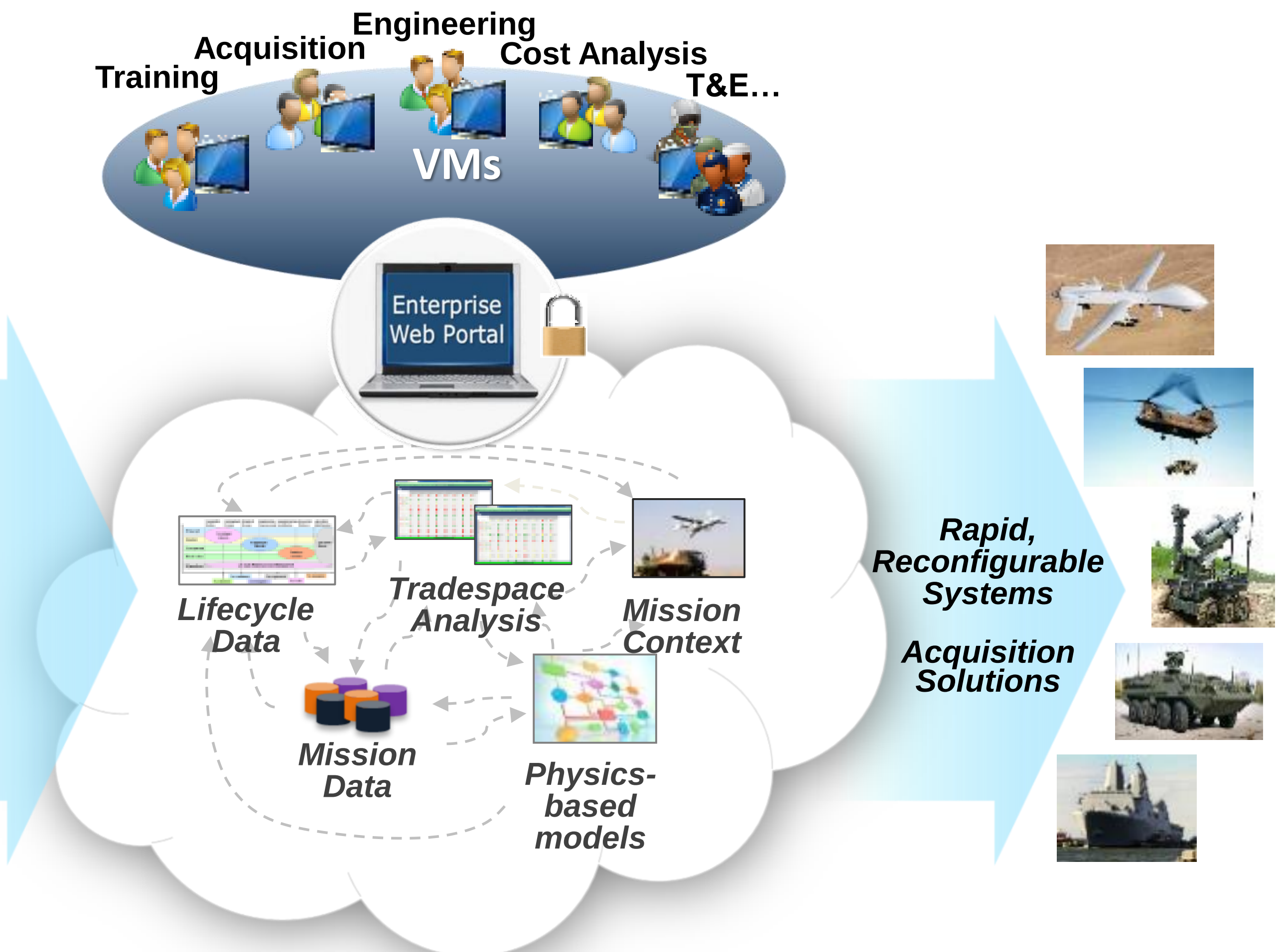
Previous Design Successes, Lessons-learned

Needs (…ilities)

- *Manufacturability*
- *Affordability*
- *Reliability*
- *Sustainability*
- *Usability*
- *Testability*
- *Etc.*

HPCMP Resources

S&T Resources, Research



Physics and Model-Based Aerodynamic Design and Analysis

Presented:

NDIA Systems Engineering 2017

October 26, 2017

GENERAL ATOMICS AERONAUTICAL

General Atomics Aeronautical Systems

Predator A
Piston
(In Production)

Predator B/C
Turboprop/fan
(Production/Dev)

Small/Large
UAVs
(In Dev)

Product Aerodynamic Lifecycle

Requirements

Conceptual Design

Prelim/Detailed Design

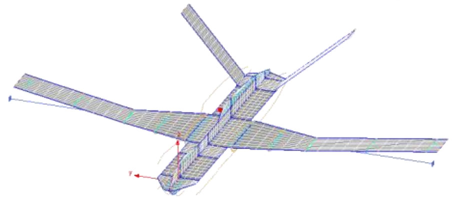
Test

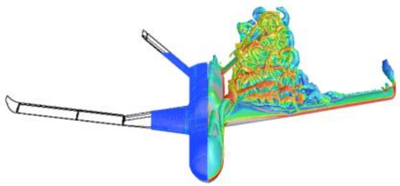
Sustainment / Growth

- **Aerodynamic design and analysis relevant to all stages of the product life cycle**
- **Ideally need a set of “multi” tools**
  - Multi-fidelity (low → high fidelity)
  - Multi-physics (aero → aero+)
  - Multi-cost (sec/min → days/weeks)
  - Multi-user/org (aero vs. struct SME)
  - Multi-product (Aircraft A vs. Aircraft B)

Aerodynamic Pre-Flight Tool belt

Physics Based



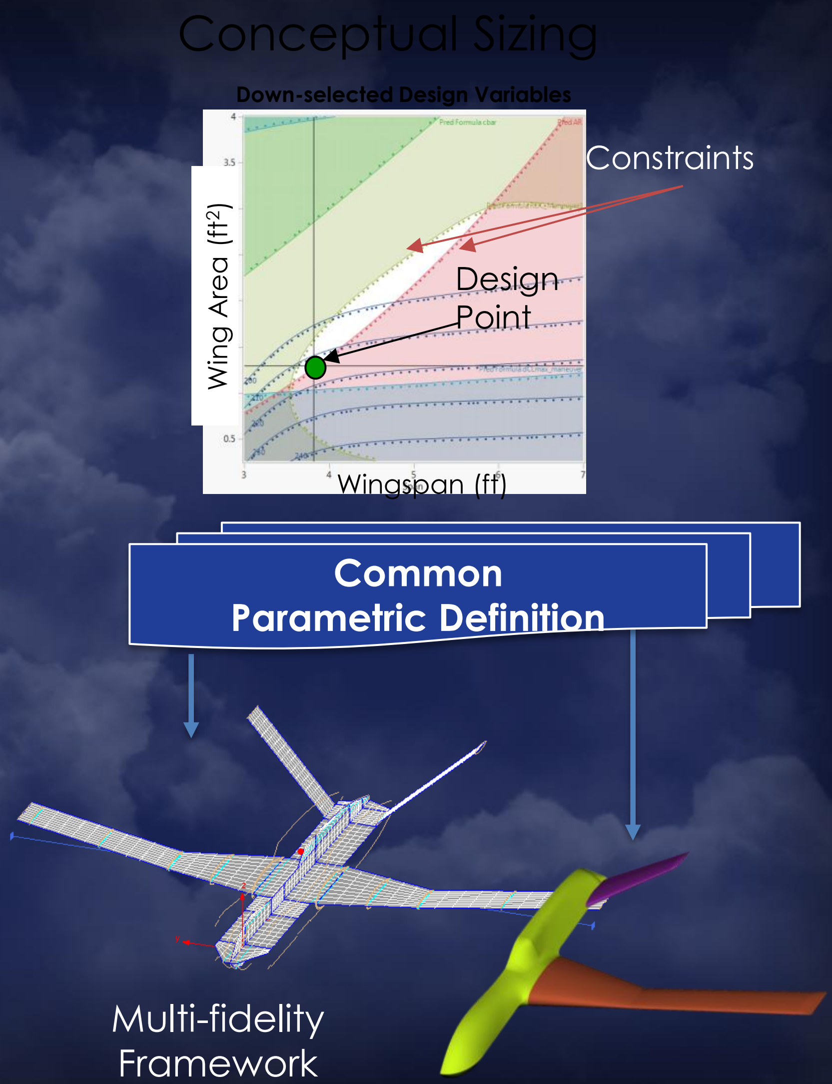


Test Based

Physics	Vortex Lattice / Panel	CFD	Wind Tunnel
Inputs	Conceptualize → Run	CAD → Mesh → Run → Post	Plan → CAD/Build → Test → Post
Outputs	**Steady/Unsteady** Linear aero **Quick** prelim results	Steady/Unsteady **Non-linear aero** **Validation required**	Typically steady aero **Non-linear aero** **Established data source**
Scale (Reynolds #)	Full-scale (Inviscid i.e. Re→∞)	**Full-Scale** (Flight Re)	Sub-scale or partial model (Variable Re adds **cost**)
Compressibility	Incompressible or compressibility corrected	Compressible (Flight Mach)	Compressible. Separate tests depending on Ma
Viscous Effects	Inviscid or viscous corrected	Typically fully turbulent Recent RANS transition models	Typically tripped or natural transition at test Re
Geometry	Panel representation and **simple shapes**	Geometric complexity increases meshing cost; smooth	Smooth; gaps/slots sizes may need to be Re scaled
Propulsion	Faired; no or limited prop effects	Faired or flow-through; can model propulsion effects	Faired or flow-through; separate tests for prop effects
Environment	Modeled in farfield	Modeled in farfield	Corrected for tunnel effects

Requirements / Conceptual Design

- **Semi-empirical methods drive requirements and sizing**
  - High level
  - Grounded in actuals
  - Good for derivative designs
  - Good for high level trades
- **Opportunities**
  - Multi-fidelity framework at GA-ASI
  - Others successfully options exist e.g. MIT TASOPT



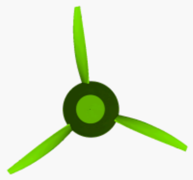
GENERAL ATOMICS AERONAUTICAL

Preliminary / Detailed Design

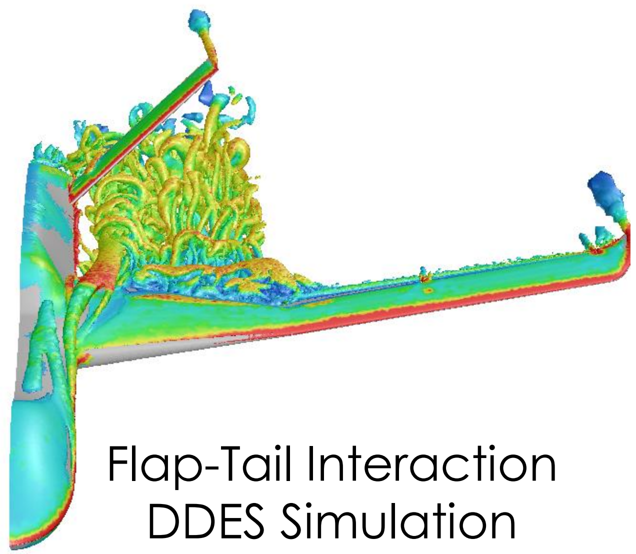
- **CFD and wind tunnel test drive design**
  - Analysis for design trades
  - Test for database generation
  - Test for perf verification
- **Challenges**
  - Managing multiple models… CREATE-AV enabling multi-disciplinary analysis
  - Physics!.. the RANS plateau LES/DDES still costly

Kestrel CFD Model

Animated gif



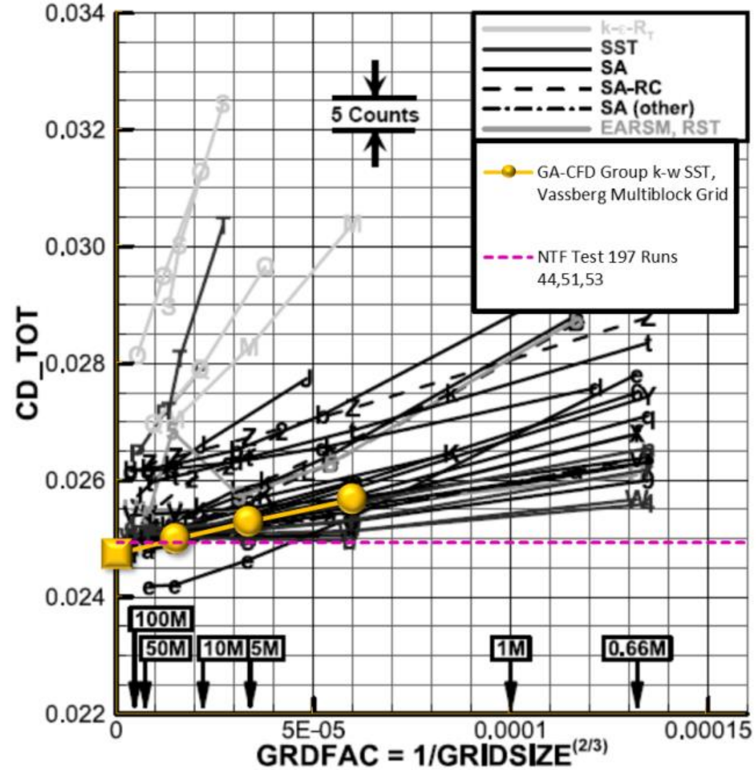
Overset allows moving control surfaces and props



Flap-Tail Interaction DDES Simulation

Prelim / Detailed Design (Cont.)

- **Challenges (Cont.)**
  - Scalability… Wind tunnel cheaper than CFD for large databases.
  - Trust… CFD meshing treated as an “art.” Mesh convergence ≠ Solution accuracy. Test validation remains essential.
  - Expectations… CFD not fast enough to be in-exact.
  - Process… CFD treated as virtual wind-tunnel.

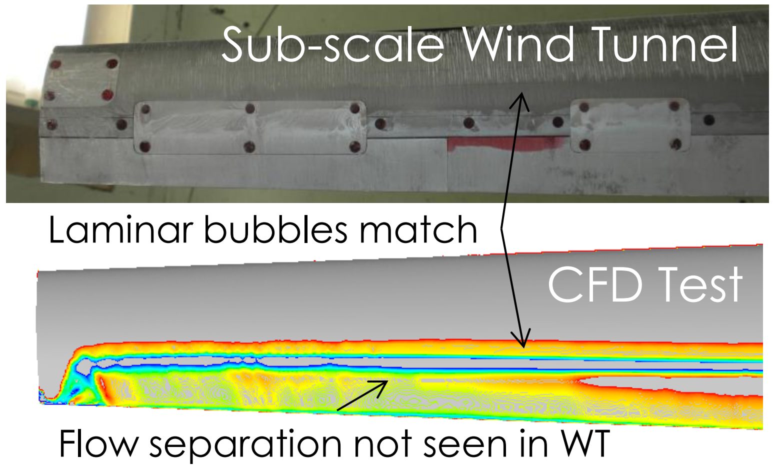


AIAA Drag Prediction Workshop (DPW5)

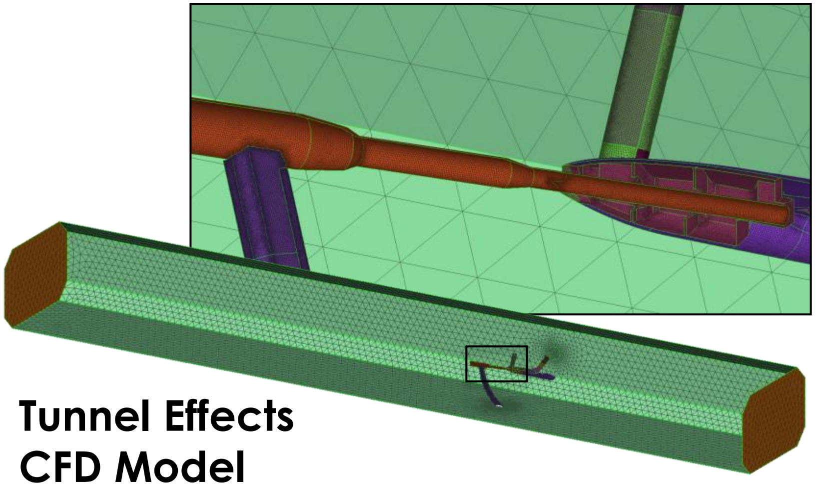
Graphic from: https://aiaa-dpw.larc.nasa.gov/Workshop5/presentations/DPW5_Presentation_Files/14_DPW5%20Summary-Draft_V7.pdf

Test

- **Pre-test predictions inform test focus areas**
- **Test helps CFD**
  - Separated flows
  - Interaction effects
  - Transition
- **CFD helps test**
  - Wind tunnel corrections
  - Propulsion effects
  - Aero-static effects



Tunnel Flow Viz Comparison



Tunnel Effects CFD Model

Graphic from: https://aiaa-dpw.larc.nasa.gov/Workshop5/presentations/DPW5_Presentation_Files/14_DPW5%20Summary-Draft_V7.pdf

Closing the Loop on Performance

Requirements

Conceptual Aero

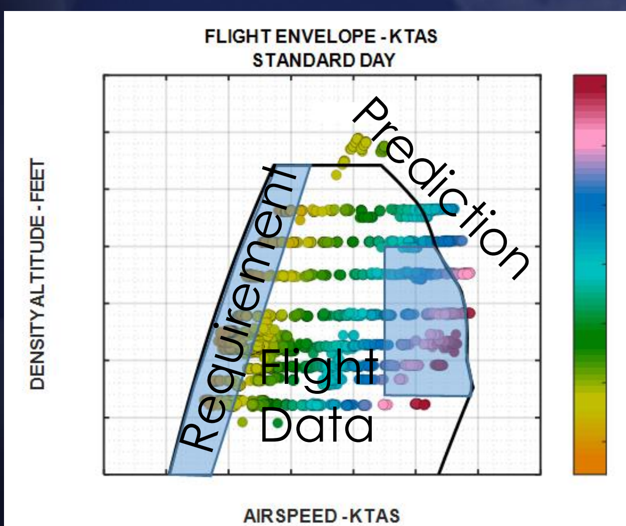
RANs Aero

Wind Tunnel Aero

Flight Test Aero

All aero models contribute to:

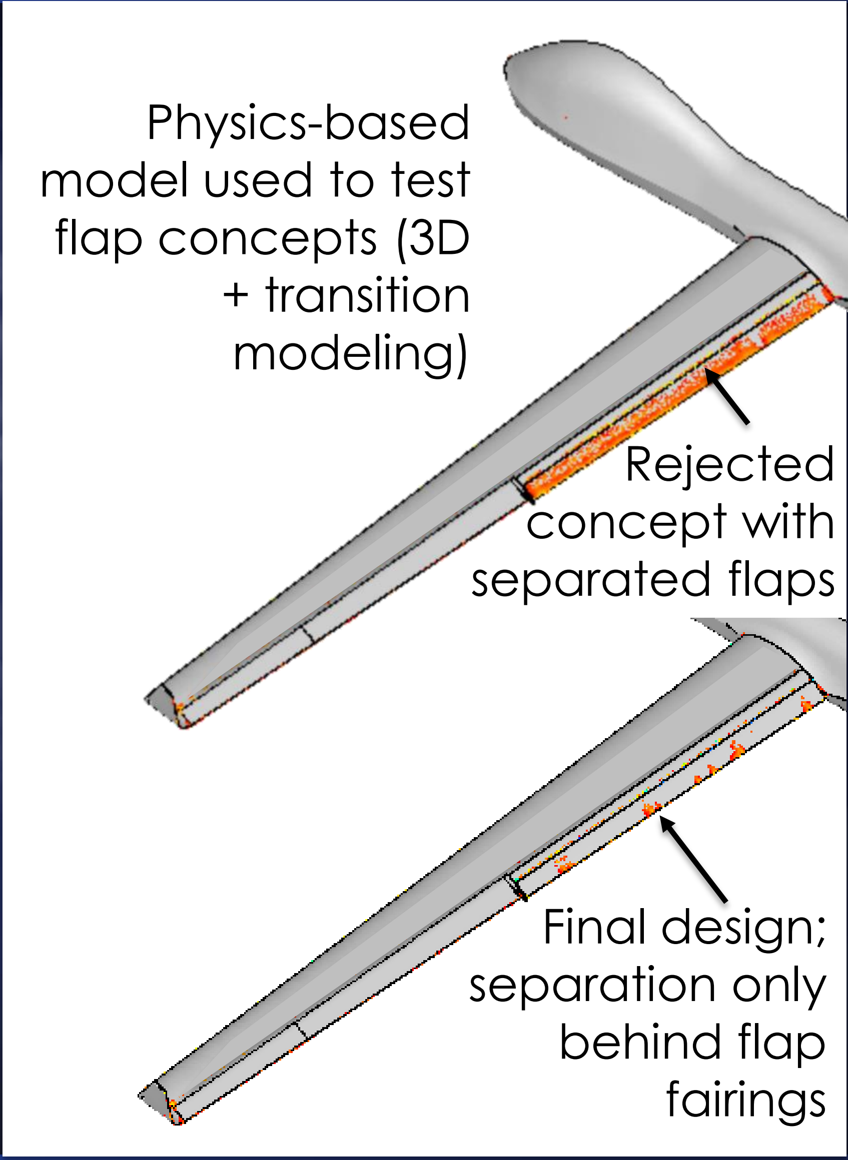
- Understanding of aircraft flow-field
- Support modeling for perf and S&C
- Air-data integration



Aero + Weights + Propulsion
= Performance

Sustainment / Growth

- **New tools provide opportunities to improve existing systems and match evolving customer needs**
- **GE → GE-ER Case Study**
  - GE double slotted flap designed with 2D CFD
  - GE-ER reconfigured existing hardware to a single slotted flap with 3D CFD
  - Wind tunnel and flight test in both cases
  - Meet current customer needs



Future Needs

- **Medium fidelity needs**
  - Fast 3D methods (can include fuselages)
  - Non-linear unsteady options (damping deriv, loads spectra)
- **Promising Candidates**
  - Coarsely auto-meshed RANS/URANS with wall functions
  - Auto-meshed Euler+IBLT3
  - Probabilistic multi-fidelity methods like Kriging
- **High fidelity needs**
  - More efficient algorithms (e.g. multi-grid)
  - Less reliance on hardware solutions (costly)
  - Faster CAD clean-up (time consuming)
- **Transition modeling essential for GA-ASI**
  - RANS based models promising from computational cost perspective
  - Need models robust to Re 5e5-10e6 (current γ-Reθ not there)
  - Natural transition covering TS, CF, laminar bubbles, attachment line contamination
  - Forced transition covering trip, surface roughness/defects
  - Non-dissipative methods for high level for freestream turbulence in RANS

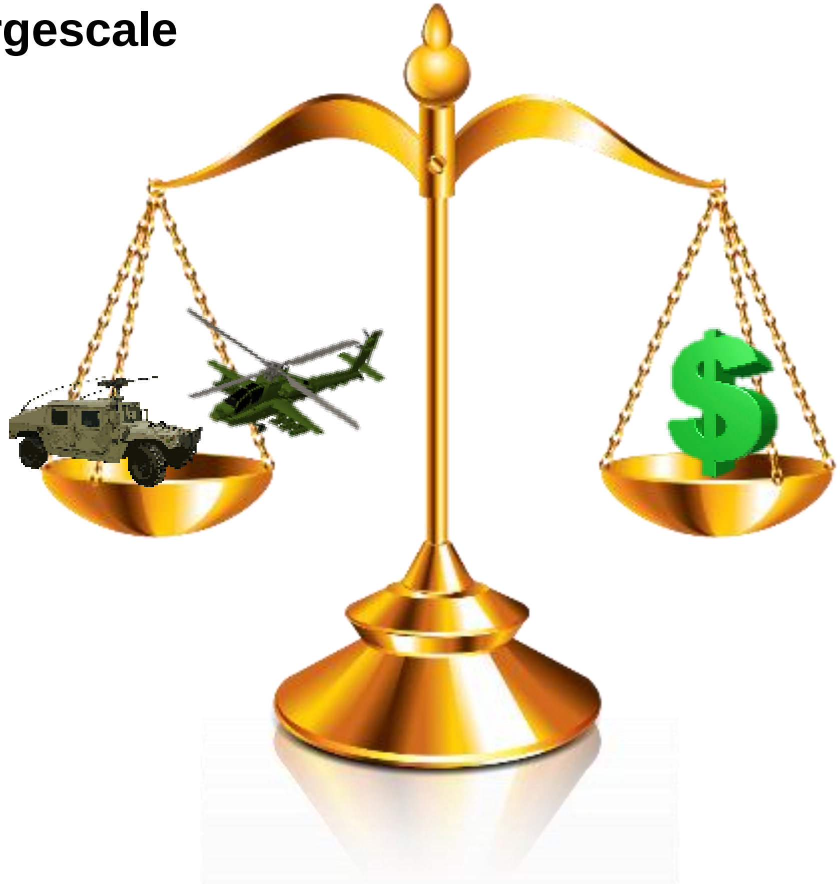
Introducing Lifecycle Cost to Early Conceptual Tradespace Exploration

20th Annual NDIA Systems Engineering Conference
October 26, 2017

E. Alex Baylot, Research Industrial Engineer
James “Jed” Richards, Operations Research Analyst
US Army ERDC

Objective and Outline

Provide ERS Lifecycle Cost (LCC) development plan and methods for linking cost models to performance models for generating largescale tradespaces



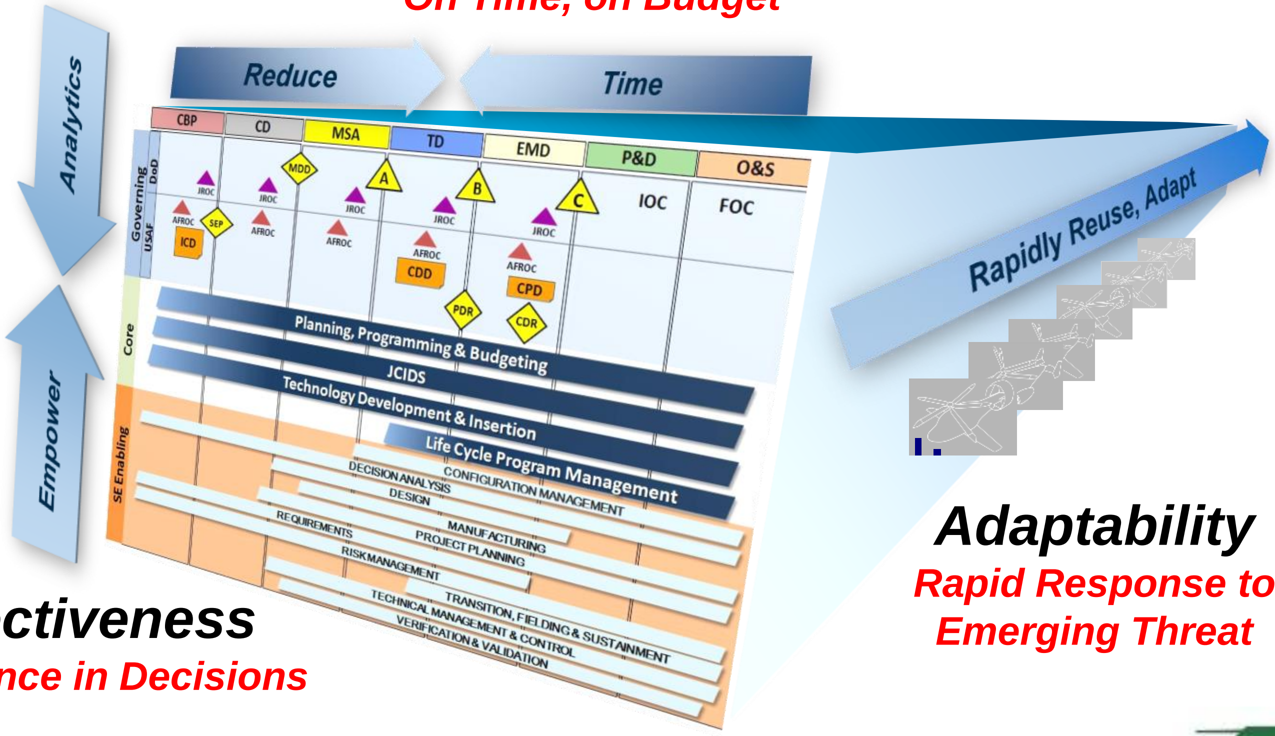
- Objective
- Background
- Cost Estimating Techniques
- Cost Analysis Use Case
- Surrogate Model Creation Method
- Low-Cost Attritable Aircraft Use Case
- ERS Cost Model Development Plan
- Summary
- Questions

Background

A goal of the Engineered Resilient Systems (ERS) Program is to create a capability for linking cost and performance models for early concept exploration of design alternatives

Affordability

On Time, on Budget



Adaptability

Rapid Response to Emerging Threat

Effectiveness

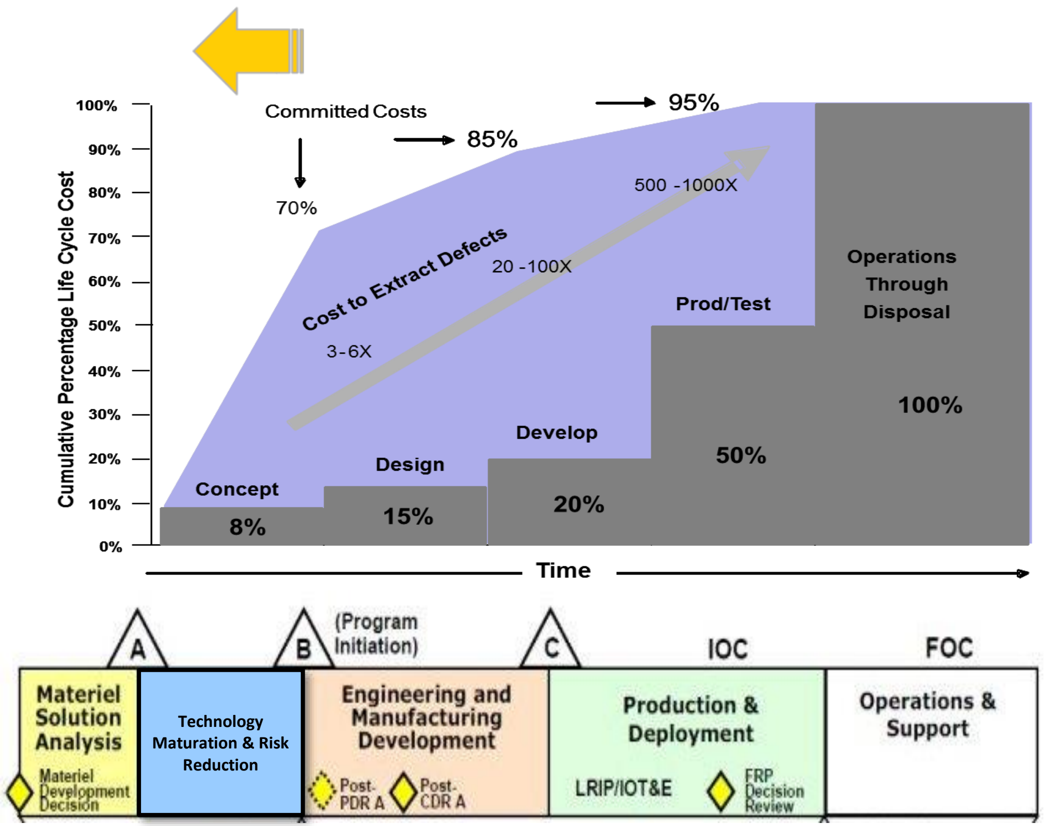
Confidence in Decisions

Background

Affordability Analysis (Pre-Milestone A/B)

- Determine Affordability Goals/Caps
- Estimate Program Lifecycle Cost
- Establish Cost Targets
- Analyze Cost/Performance Trades

Committed Lifecycle Cost



Reference DoDI 5000.02 Defense Acquisition Life Cycle Compliance Baseline

Cost Estimating Techniques

Analogy

- Quick, inexpensive, easy-to-change
- Subjective, not precise, poor comparison between new and old systems
- Typically used pre-Milestone A through Milestone A

Parametric

- Cost estimating relationships, inexpensive, easy to do “what-if” drills
- Moderately subjective, precision only as good as databases
- Typically used pre-Milestone A through Milestone B

Engineering

- Very accurate in later stages of EMD, limited subjectivity, uses WBS
- Very expensive, very time consuming, “what-ifs” are difficult
- Typically used Milestone B through post-Milestone C

Actual Costs

- Limited subjectivity, very accurate
- Limited actual cost data, very expensive, very time consuming, “what-ifs” are difficult
- Typically used Milestone C through post-Milestone C

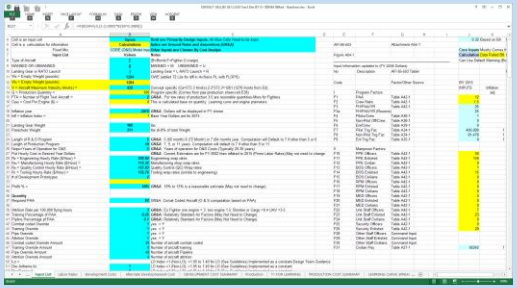
DAU ACQ 101

Cost Analysis Use Cases

	Use Cases	ERS Partner
Create/Adapt Cost Model	1 – Manual CER: User manually enters Cost Estimating Relationships (CER) to build a cost model	UAS (NCCA, UAS Handbook)
	2 – Existing Menu: User choses an existing cost constraint component and adjusts (calibrates) for specific cost generation	Helicopter (GTRI, Commercial rotorcraft cost model)
	3 – Historic Cost Data: cost model from user provided historic cost data	Ground Vehicle (TACOM, CADE data)
Link Existing Cost Model	4 – Existing Model Surrogate: Allows user to provide an existing cost data set derived from any source to generate meta model for cost domain tradespace generation (surrogate cost modeling)	Surface Ship (NSWC Carderock, Surface Combatant Performance Based Cost Model)
	5 – Excel Cost Model: Allows user to provide an existing excel based cost model to link to tradespace generation	Un-Manned Aircraft (AFRL – LCAAT)
	6 – COTS Cost Model: User provides a COTS integrated tools model	[development pending]

Surrogate Model Creation Method

Connecting cost models to other tradespace models



Python Wrapper/Parser

I/O
Combinations

Surrogate Model

+100K

Use existing spreadsheet cost model

Use Monte-Carlo techniques

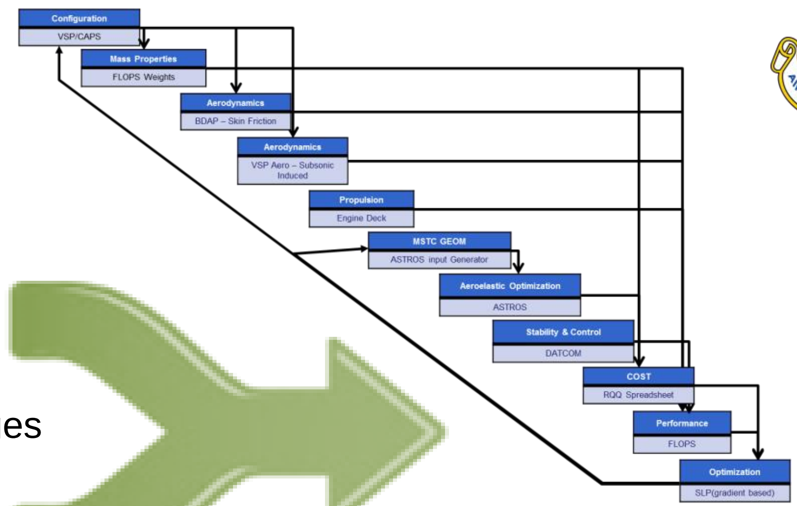
Generate surrogate-regression model

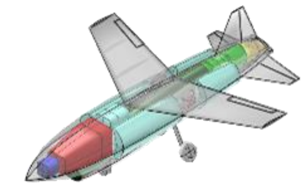
Low-Cost Attritable Aircraft Use Case

Current Method*

Computer-language cost model derived from spreadsheet to MATLAB or Python

- 4 months development
- Slow response to changes





- ❑ Aeroelasticity
- ❑ Structural sizing
- ❑ Cost
- ❑ Stability & Control
- ❑ Multi-Fidelity
- ❑ Parametric Analysis Optimization

Surrogate Method

Surrogate Model

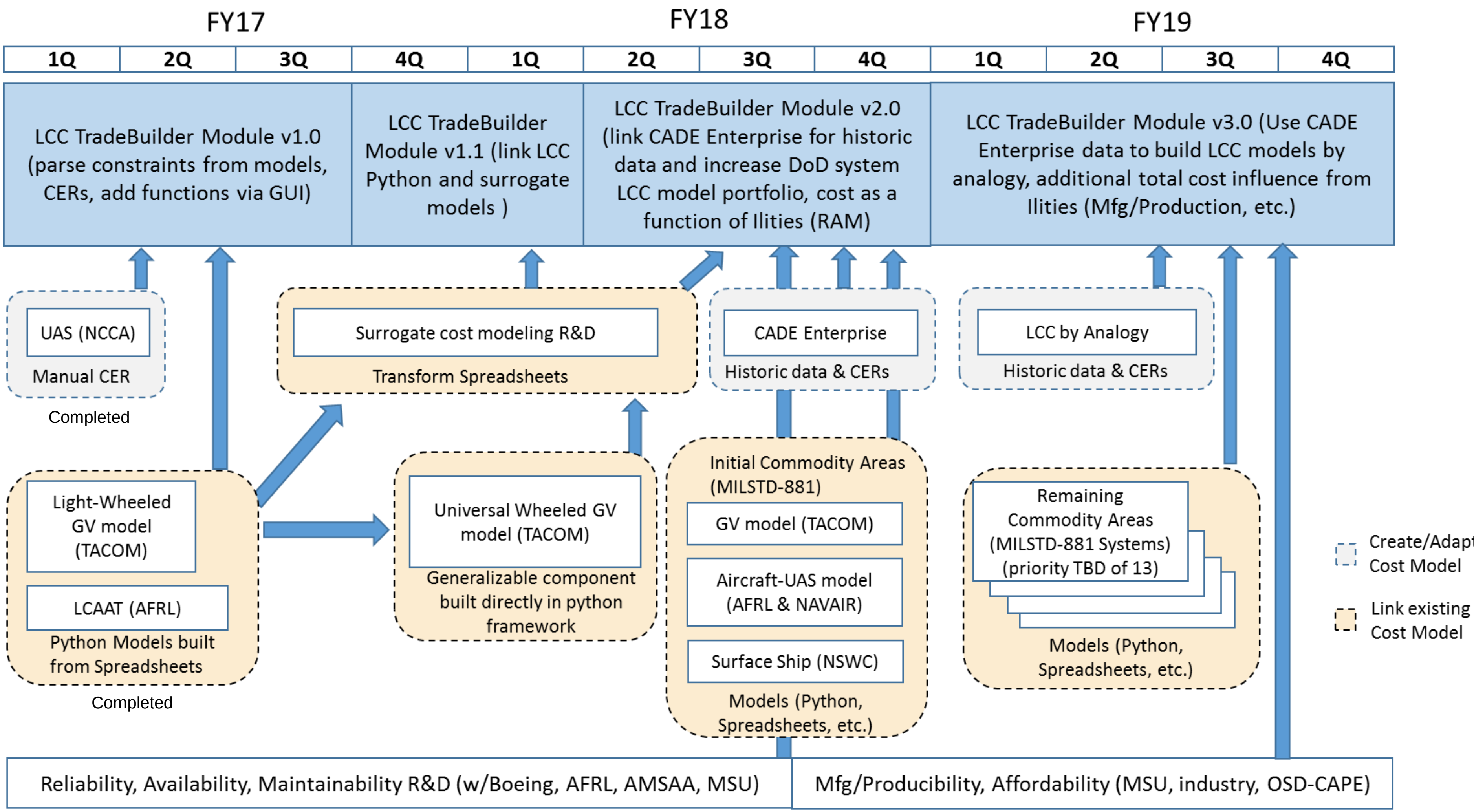
- 24 hours development
- Quick response to changes

100X reduction in cost model integration period

Model Execution

*Not typical

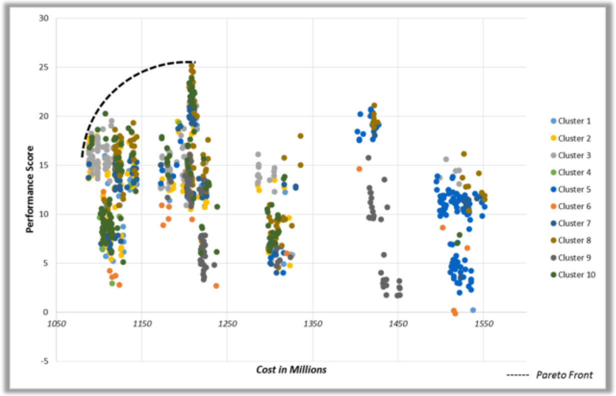
ERS Cost Model Development Plan



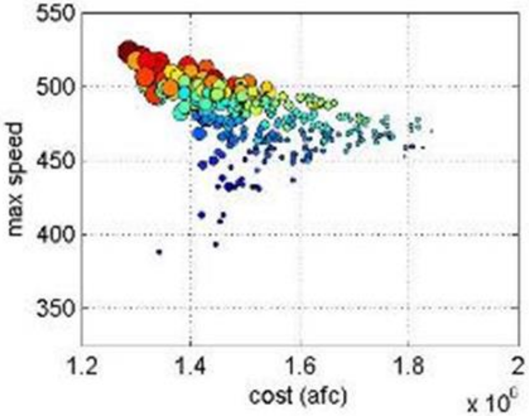
Summary

- DoDI 5000.02 identifies the requirement at Milestone (MS) A for an Affordability analysis in addition to a cost analysis and is driving more accurate cost analysis to the left
- ERS is developing methods to better integrate cost models into conceptual tradespace exploration using existing models or surrogate models
- Surrogate modeling methods show promise to greatly accelerate the integration process into tradespace exploration for pre-MS A & at MS A
- The ERS cost model development plan strives to provide a capability for all system commodities supporting all Services and OSD-CAPE

Ground Vehicle



UAS



Questions

Mr. E. Alex Baylot, US Army ERDC
Alex.Baylot@usace.army.mil

Mr. James “Jed” Richards, US Army ERDC
James.E.Richards@erdc.dren.mil

ERS NDIA
FUELING INNOVATION & COLLABORATION

An Adaptive Automation Approach for UAV UI Concept Development

Jeff O'Hara, Senior Research Scientist
Stuart Michelson, Research Engineer II
Georgia Tech Research Institute,
Human Systems Engineering Branch

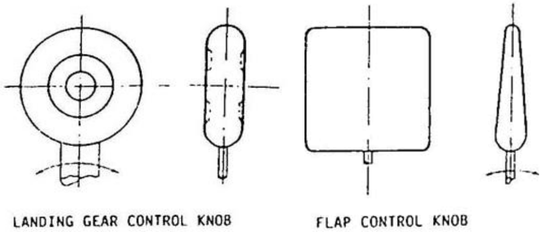
NDIA Systems Engineering Conference
24OCT2017

Georgia Tech Research Institute
Problem. Solved.

Background

- High loss rate of U.S. Military UAVs
- Numerous ergonomic / automation causal factors (Source: USAF SAB):
  - 80% of Predator mishaps involved human error due to fundamental design issues.
  - Warning/status messages buried layers deep.
  - Complex automation (22 steps to turn on the autopilot on the Predator).
  - $4.5M Predator lost due to pilot accidentally selected the engine kill switch instead of the landing gear switch.
- Analogous in terms of maturity to early manned cockpit design (systematic control shape coding analyses fixed a spate of B-17/B-25 crashes).
- Need a Systems Engineering approach to higher order human/automation system design.

B-17 Flap and Gear Handle



Modern Shape Coding

Challenging Emergent Requirements Driving the Need for Automation

Georgia Tech Research Institute

- New UAV Combat Missions:
  - Airborne Electronic Attack (AEA)
  - Air to Ground (A/G)
  - Air to Air (A/A)
- New User Interface Goals:
  - Single Pilot for multiple UAVs
  - Multiple user interactions (ground troops, manned air).

UAV kill by Tactical High Energy Laser (THEL) 2011

- Derived Requirements Mandate the use of Automation:
  - Single pilot mismatch with available attention span over multiple vehicles and multiple users.
  - Human reaction time mismatch (reactive jamming of enemy radar pushes automated response requirements)
  - Human computational limit reached (pilot is overmatched trying to compute fuel burn vs. rerouting requirements for signature management, etc.).

UAV Current Automated Capability

UAV: “an aircraft or balloon that does not carry a human operator and is capable of flight under remote control or autonomous programming.”

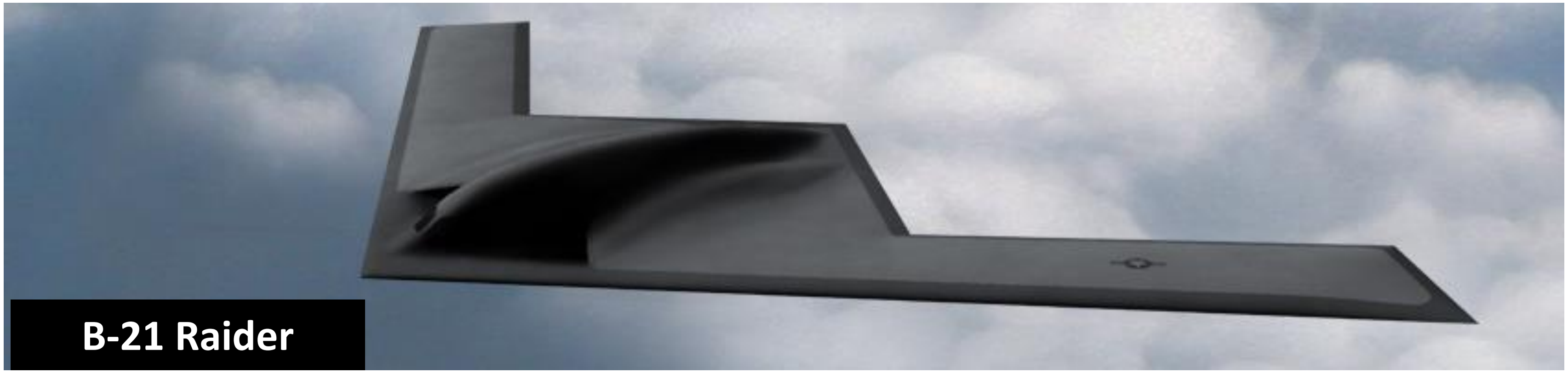
(US DoD Definition: JP 1-02)

- Current UAVs have very limited autonomy (e.g. preprogrammed flight to regain a lost link, auto land).
- Designers are struggling with adding more, incrementally.

MQ-1 Predator GCS

What to Automate – and what to NOT.

- The appropriate Systems Engineering question is not “how to design man out”, but rather “which functions and tasks are appropriate to automate, and how?”.
- Factors include:
  - Tactically significant timelines
  - Latency in the control loop (Observe/Orient/Decide/Act – OODA)
  - Need for human oversight and control – with weapons releases.



- The next step is to recognize the need for automation to manage automation itself.

Operator Role Theory of Automation
(Folds, 1995)

NO EQUIPMENT IN THE LOOP → INCREASING USE OF AUTOMATION → NO OPERATOR IN THE LOOP

"DIRECT PERFORMER" REGION

- HUMAN CLOSES LOOP
- CONTROL LOOP COMPONENTS PREDOMINANTLY HUMAN

"MANUAL CONTROLLER" REGION

- HUMAN CLOSES LOOP
- CONTROL LOOP COMPONENTS ARE A MIXTURE OF HUMAN AND MACHINE

"SUPERVISORY CONTROLLER" REGION

- HUMAN OR MACHINE CLOSES LOOP
- CONTROL LOOP COMPONENTS ARE PREDOMINANTLY MACHINE

"EXECUTIVE CONTROLLER" REGION

- MACHINE CLOSES LOOP
- CONTROL LOOP COMPONENTS ARE MACHINE ONLY
- HUMAN MAY START OR STOP FUNCTION

System of Systems Approach

Georgia Tech Research Institute

- Need a system of systems engineering approach across applications - to adaptive automation.
- Perform MTA/Task Decomposition and apply Operator Role Theory to determine mission elements.
- Determine which elements will exceed human spans of capability.
- Determine the modes of interaction between automation, and the overarching control loop tasks.
- Determine where **Executive level automation** is best suited to arbitrate or interpolate or monitor, and where the tasks are best suited for humans.

Executive Agent Example

Georgia Tech Research Institute

The Executive Agent

- Monitors automation managers within UAVs.
- Monitors coordinated tactics across UAV platforms.
- Compares weighted impacts of conflicting automation.
- Auto performs defined tasks / alerts pilot for other tasks.

+ N

The Datalink Manager

- Monitors datalink latency and quality against calculated range.
- Multiple links (UAV/UAV, UAV/manned, UAV/GCS, etc.)
- Alerts when nearing lost link.
- Sets flight path to regain link.

The Signature Manager

- Monitors ownship multispectral vis against known threat sensors.
- Continuously computed during maneuvering.
- Alerts when near high Pd.
- Sets flight path to avoid.

Executive Agent With the OODA Loop

Georgia Tech Research Institute

- Monitor (“Observe/Orient”)
- Adjudicate (“Decide”).
- Recommend (or “Act”).
- Inform: elevate urgent advisories (would inform, then prompt, then warn).
- Perform specific-to-general reasoning related to induction, synthesis, and integration tasks.
- Perform general-to-specific reasoning related to deduction, analysis, and differentiation.
- Return the pilot to the role of a tactician.

Summary

Georgia Tech Research Institute

- The piecemeal use of automation may be worse than having none.
- By equipping proposed future multiple combat UAV control systems with agile, Executive level controllers which can rapidly perform multivariate, weighted arbitrations between systematically integrated automation, time critical combat tasks can be met within the multiple UAV control paradigm.

An Adaptive Automation Approach for UAV UI Concept Development

Jeff O'Hara
404-407-8507
Jeffrey.ohara@gtri.gatech.edu

Stuart Michelson
404-407-6162
stuart.michelson@gtri.gatech.edu

Georgia Tech Research Institute
Electronic Systems Laboratory
400 Tenth St. NW
Atlanta, GA 30332-0840

Abstract

Despite decades of industry experience in the design of Unmanned Aerial Vehicle (UAV) control systems and their user interfaces, a combination of factors persist that produce a significant and unacceptable loss rate of UAVs due to poor user interfaces. One significant element is the current focus of human systems design on lower-order User Interfaces (UI) at the expense of investing in the design of an adaptive higher level integration to relieve inattentive or overtaxed operators of significant functionality as required, and to perform time-critical tactical tasks which humans cannot perform or for which they are not well suited. The approach proposed is one which defines the respective roles of user interactions with adaptive policy manager automation to address the loss of vehicles and mission failures. Specific policy manager automation elements are explored which will enable the system to flexibly assume or release UAV vehicle or systems functionality based on operator action/saturation in a number of mission areas. A notional Executive automation controller design approach is outlined to meet time critical information integration and mission task requirements.

Introduction and Historical Background

Despite decades of industry experience in the design of Unmanned Aerial Vehicle (UAV) control systems and their user interfaces, a combination of factors persist that produce a significant and unacceptable loss rate of UAVs due to poor user interfaces. By way of comparison to the progression of manned aircraft pilot vehicle interfaces, the UAV UI field has failed to progress as rapidly, being somewhat stalled at an equivalent of a 1940's state of the art with design foci on improved detailed level UI (menus, knobs, switches, screens), rather than on addressing systematic higher order user-system automation design.

In the 1940s, manned aircraft human engineering underwent a radical change in design philosophy with the work of human factors engineering pioneers such as Alphonse Chapanis, who applied engineering psychology to correct basic cockpit design flaws. The classic example of application of early engineering psychology analyses is the effort to mitigate a rash of bomber gear up crash landings. Human factors engineers redesigned landing gear handles to be shaped like wheels and reshaped flap handles shaped like flap handles for tactile discriminability by pilots who were visually focused on performing landing tasks. These were point design solutions, but were systematically applied through the cockpit and were eventually incorporated into the military standard system (Roscoe, 1995).

A systematic review in 2011 by the U.S. Air Force Scientific Advisory Board found a number of significant ergonomics and automation deficiencies in several current UAV Ground Control Systems (GCS), including poorly mechanized autopilot interfaces as well as “classic” pilot vehicle interface deficiencies. One example recalled the 1945 bomber crashes; the crash of one \$4.5 million Predator UAV was directly caused by a pilot mistakenly choosing the “kill engine” switch instead of the adjacent landing gear switch (Morely, 2012). That a Predator pilot was even able to mistake (let alone be allowed to actuate in flight) the "kill engine" switch for the landing gear switch would seem to indicate the lack of a systems engineering analytical approach to user interface requirement definition.

Other studies have confirmed the apparent lack of a systematic design approach. A 2007 Air Force Research Lab study found that up to 80% of Predator mishaps alone involved human error, including poor documentation, crew coordination mistakes and training, and serious fundamental human factors design issues with GCSs. For example, it apparently took 22 key strokes to turn on the autopilot on early Predators; warning, caution and advisory messages were buried under layers of noncritical interfaces, resulting in situations where the pilot receives few if any alerting cues to emergencies. More than 400 US UAVs have crashed since 2001 (including midair collisions) and due to these causes, which contributed to lack of pilot awareness of or correct responses to weather, fuel status, data link strength, and high terrain (Craig, 2012).

Looking forward, UAV missions are expanding and multiplying into roles (such as Airborne Electronic Attack and Air to Air engagements) which stress rapidity of decision making in a complex shifting combat environment. Emergent warfighter UAV design goals are trending toward requirements for single user command and control of multiple heterogeneous UAV platforms with separate mission taskings, as well as requirements for cooperative control between a GCS and an off board user (such as a front line soldier or pilot). A Human Systems Integration (HSI) design approach limited to lower order point design switch and display issues or merely complying with military standard compliance audits does not address the systems engineering challenges from these needs. These new requirements present more challenging problems such as issues with single user task saturation and vigilance and how user system automation can augment a human user to prevent mishaps and enable mission success. This paper will summarize an approach to provide a framework for an adaptive, operator centric automation framework for future and retrofit naval UAV designs.

The approach recommended is two faceted; the first is the need for individual, adaptive automated policy managers focused on specific mission tasks (especially those needing rapid calculation or constant monitoring). The second is the need for an overarching Executive manager to provide rapid arbitration and coordination during time-critical combat operations. The end goal is to return the user to the role of tactician, automating first order calculations (e.g. fuel, terrain avoidance) but with a higher order automated process to ensure a coordinated response to human tactical direction.

Progress towards Adaptive GCS Automation

Two historically prevalent approaches to UAV GCS design have been followed. One approach focused on provision of controls duplicating manned aircraft interfaces (e.g. the approach used from 1940's designs up through the MQ-1 Predator). The other provided direction of the vehicle through graphical map cues (evolving from hard copy strip charts to present day point and click graphical interfaces to direct flight to a point). Either approach offers the potential for the uncoordinated application of multiple instances of automation (e.g., an automated route planner will disagree with an automated terrain avoidance system – and will present disharmonious results to the user from separate displays). The risk, then, is that attempts to add automation to GCS designs (within either design paradigm) will impose additional new tasks and roles on the user to monitor multiple automated systems across multiple vehicles, thus increasing the risk of significant error. For example, trending UAS human errors have been noted to include (Johnson, 2007):

1. Loss of operator situational awareness (SA) of airspace and traffic.
2. Operator-induced Air Vehicle loss of fuel/loss of link, leading to vehicle loss.
3. Loss of operator SA of altitude, airspeed, vehicle status, and clearance to terrain.

Operator Role Theory (Folds, 1995) posits a spectrum of human and automation shared roles in systems control (see Figure 1, below). Where no automation is present, the user is acting in a "Direct Performer" situation. With automation present but with the user performing information synthesis and control of the system, the system is running in a "Manual Control" region. With predominantly automated control loop processes and user monitoring and adjustment, the system is in a "Supervisory Controller" region, and finally, in the "Executive Controller" region of automation, the human is not in the control loop at all, save for a start/stop function

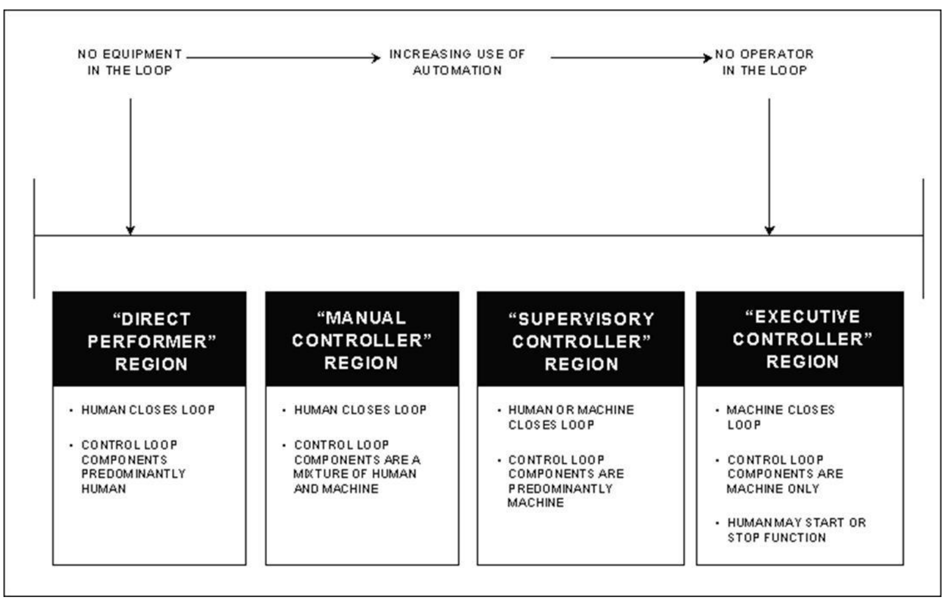


Figure 1 Continuum of Operator and Automation Roles

The classic example of Executive level control is cell phone tower switching, which takes place at an Executive level (human interaction with this automated element is generally limited to seeing the signal strength bar on their phone). Currently, GCS designs incorporate a mix of automation from in various automation control regions, with varying success. The move towards multiple UAV GCS control will only exacerbate existing problems without adoption of a new element of automation to aid the user in automation management. Newer GCS designs are undertaking to provide adaptive automaton which provides tools for automatic flight routing, route deconfliction, and calculation of weapons engagement zones, SAM shot avoidance cues, and so forth based on integrated "at a glance" presentations (Johnson, 2007).

Mission Growth Forces an Approach with an Executive

As with the cell phone example, the Executive automation role is well proven in manned combat aircraft. Airborne electronic warfare jammers react immediately, for example, to defeat incoming enemy missiles by automatically applying radar jamming techniques. The system executes the protective action because the pilot doesn't have the reaction time (let alone the surplus workload capacity) to manually employ the equipment. Particularly for pilots who may be tired or inattentive, the sudden leap in activation from being a system monitor to dealing with an emergency can lead to lapses and errors. Thus, a higher level requirement exists for a controller capability which looks across automated subsystems for multiple UAVs, accessing data to predictively analyze trends and threats in a coordinated manner, without the potential for boredom or fatigue.

To match the required UAV UI demands, a comprehensive shift to a system of systems engineering approach to adaptive automation – across applications – is recommended. With multiple UAVs aloft in a highly dynamic battlespace (where UAVs may be used not just for long counterinsurgency patrols, but as targeting and/or weapons platforms in air to air combat), automation needs to be considered as more than a family of decision making tools, but as an integrated system itself. A human systems engineering approach which applies operator role theory (Folds, 1995) to define a UAV system of systems will effect an order of magnitude improvement in combat efficiency and effectiveness. The approach proposed specifically advances the definition of multi-mission adaptive automation to address the impacts of (1) highly complex mission tasking (2) too many vehicles to manually monitor at once and (3) short engagement timelines.

Elements of the Integrated Solution: Policy Managers and an Executive

Automation should relieve humans from boring housekeeping tasks, prevent their inattention or raw information saturation from causing loss of vehicle and mission failure conditions, and allow humans to do that which they do best (make tactical judgments). Specific automation "policy" managers should be considered for collaborative integration in a fused GCS implementation. Many automation elements have already been fielded as separate tools in manned and unmanned aircraft. However, to implement enough of them, over multiple UAVs, with newly emergent requirements for tactical engagement accuracies and timelines, additional Executive level automation is needed.

Each policy manager has a role to play as individual automated elements under an Executive, which would supplement the monitoring and arbitration task set currently allocated to the human. An Executive would be able to quantitatively perform that role across multiple UAVs, and would be able to meet far tighter accuracy and speed requirements. The Executive must be able to resolve a best fit solution for the active UAV platforms given preplanned mission constraints by performing multivariate, weighted, arbitrations across the lines of the subordinate policy managers. Example potential individual automation elements include Auto Ground Collision Avoidance System (AGCAS) Protection, Auto Traffic Collision Avoidance Protection, Auto Envelope Protection, Auto Airspace Protection, Auto Datalink Protection and Auto Signature Protection (among a host of other functions). It is useful to examine how two (a Datalink Manager and a Signature Manager) interact.

The Datalink Manager monitors established UAV to GCS, UAV to UAV, and UAV to manned mission partner datalink latency and strength against calculated range limits. It then provides a real time calculated assessment of the probability of loss of link(s) as well as quality factors. (Link latency, as an example quality factor, will impact the ability of the vehicle to perform time critical tactical tasks). Based on this, as well as the availability of alternative links, this policy manager automatically shifts and configures data links In an integrated automation system, the Datalink policy manager will need arbitration with the Signature and other managers to regain signal while ensuring the "lost" AV avoids maneuvers which compromise detection or survivability.

The Auto Signature Protection manager provides real time computed signature management to ensure that the UAV remains either undetected or unengageable by threat systems. Based on preplanned settings, the Signature policy manager would provide a spectrum of adaptive actions from advisories to cautions to warnings to auto heading/alt changes based on flight paths past the minimum allowable approach range toward threats. This automation manager would consider the use of terrain and range line of sight effects in making an aspect/course/altitude change input; the signature policy manager would (in the proposed integrated system) make inputs in favor of or against course changes (whether automated or manual) to ensure that requested courses would not inadvertently generate a fatal shot solution from an enemy missile site. Yet obviously, some third party agent is necessary to perform the rapid, multivariate comparison and arbitration tasks between all these agents, if a human cannot possibly interpolate and calculate quickly enough.

The Need for an Executive Agent

While separately, individual automation elements may be useful, the emergence of far more complex combat requirements requires users to interpolate and integrate the many information variables (such as signature, envelope, and fuel as well as datalinks and weapons control) for multiple controlled UAVs, during multiple weapon engagements with hostile moving targets. USAF Colonel John Boyd, father of the Observe, Orient, Decide, and Act (OODA) loop model of tactical engagement, noted that the key to combat aircraft survival and autonomy is the ability to adapt to change rapidly and to capitalize on calculated advantages faster than one's opponent – to "get within the enemy's OODA loop" (Boyd, 1976). With such a varied range of automated policy managers, conflict arbitration via human or automated means is necessary. Because a single human cannot meet the analytical and computational requirement to comparatively perform the cross application functions for multiple UAVs within a tactically significant timeline for multiple controlled vehicles, the GCS must be equipped with an overarching Executive Agent.

Such an Executive would constantly monitor the individual policy managers for each UAV and adjudicate recommended automated actions based on preplanned algorithmic responses for most cases; the Executive would both provide more urgent advisories (would inform, then prompt, then warn) to cue user intervention based on the severity of impact of the problem within a tactically significant timeline (e.g. the UAV is headed for a threat, turn the UAV to avoid detection, and finally maneuver the UAV to defeat an engagement). In Boyd's terms, the control loop authority (human or Executive) must perform general-to-specific reasoning - deduction, analysis, and differentiation, while also performing specific-to general reasoning related to induction, synthesis, and integration tasks (Boyd, 1976).

In most cases, the Executive would employ hierarchical weightings to arbitrate between conflicting policy managers to prioritize actions emphasizing one mission aspect over another (such as a prioritizing lack of UAV detection over choosing the most fuel-efficient return route). In all cases, Executive arbitration of the policy managers would follow mission constraint settings selected during mission planning by the user (even if only for default settings) and consent for key tasks (e.g. weapons free status within approved engagement constraints) would necessarily be required.

Conclusion

By equipping proposed future multiple combat UAV controlling systems with agile, Executive level controllers which can rapidly perform multivariate, weighted, arbitrations, time critical combat tasks be met within the multiple UAV control paradigm. Significant further mission task analysis and requirements decomposition is necessary to ensure that further platform specific top level and detailed level design requirements are properly decomposed and allocated.

Works Cited

Boyd, John R. "Destruction and Creation". (3 September 1976).U.S. Army Command and General Staff College.

Folds, Dennis, and Mitta, Deborah. "Using Operator Role Theory to Guide Function Allocation in System Development", Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 1 October 1995.

Johnson, R, et al. "Testing Adaptive Levels of Automation (ALOA) for UAV Supervisory Control" (March 2007). AFRL-HE-WP-TR-2007-0068. OR Concepts Applied (ORCA) for Air Force Research Laboratory, Human Effectiveness Directorate, Wright Patterson AFB OH 45433.

Michelson, Stuart. "A survey of the human-centered approach to micro air vehicles". Chapter 90, Springer Handbook of Unmanned Aerial Vehicles 2013.

http://www.springerreference.com/docs/navigation.do?m=Handbook+of+Unmanned+Aerial+Vehicles+(Engineering)-book256

Morely, Jefferson. "Boredom, terror, deadly mistakes: Secrets of the new drone war". Salon.com, 3 April 2012.

http://www.salon.com/2012/04/03/boredom_terror_deadly_mistakes_secrets_of_the_new_drone_war/

Roscoe, Stanley. "The Adolescence of Engineering Psychology", Volume 1, 1997, Human Factors History Monograph Series, Steven M. Casey, Editor, the Human Factors and Ergonomics Society, Santa Monica CA.

Whitlock, Craig. "Drone crashes mount at civilian airports". Washington Post, 30 November 2012.
http://www.washingtonpost.com/world/national-security/drone-crashes-mount-at-civilian-airports-overseas/2012/11/30/e75a13e4-3a39-11e2-83f9-fb7ac9b29fad_story.html

Free and Open Source Tools to Assess Software Reliability and Security

Vidhyashree Nagaraju, Venkateswaran Shekar, Thierry Wandji[2] and Lance Fiondella[1]

[1]*University of Massachusetts*, North Dartmouth, MA 02747

[2]*Naval Air Systems Command*, Patuxent River, MD 20670

Questions?

Outline

- Year I deliverables summary
- Guidance
- Software Failure and Reliability Assessment Tool (SFRAT)
  - Architecture
  - Review of Year I functionality
  - Year II functionality
- Software Defect Estimation Tool (SweET)
- Goals

State of software reliability

- Software reliability studied for 50+ years
  - Methods have not gained widespread use
    - Disconnect between research and practice
- Diverse set of stakeholders
  - Reliability engineers
    - May lack software development experience
  - Software engineers
    - May be unfamiliar with methods to predict software reliability

YEAR I (3/15-2/16) DELIVERABLE SUMMARY

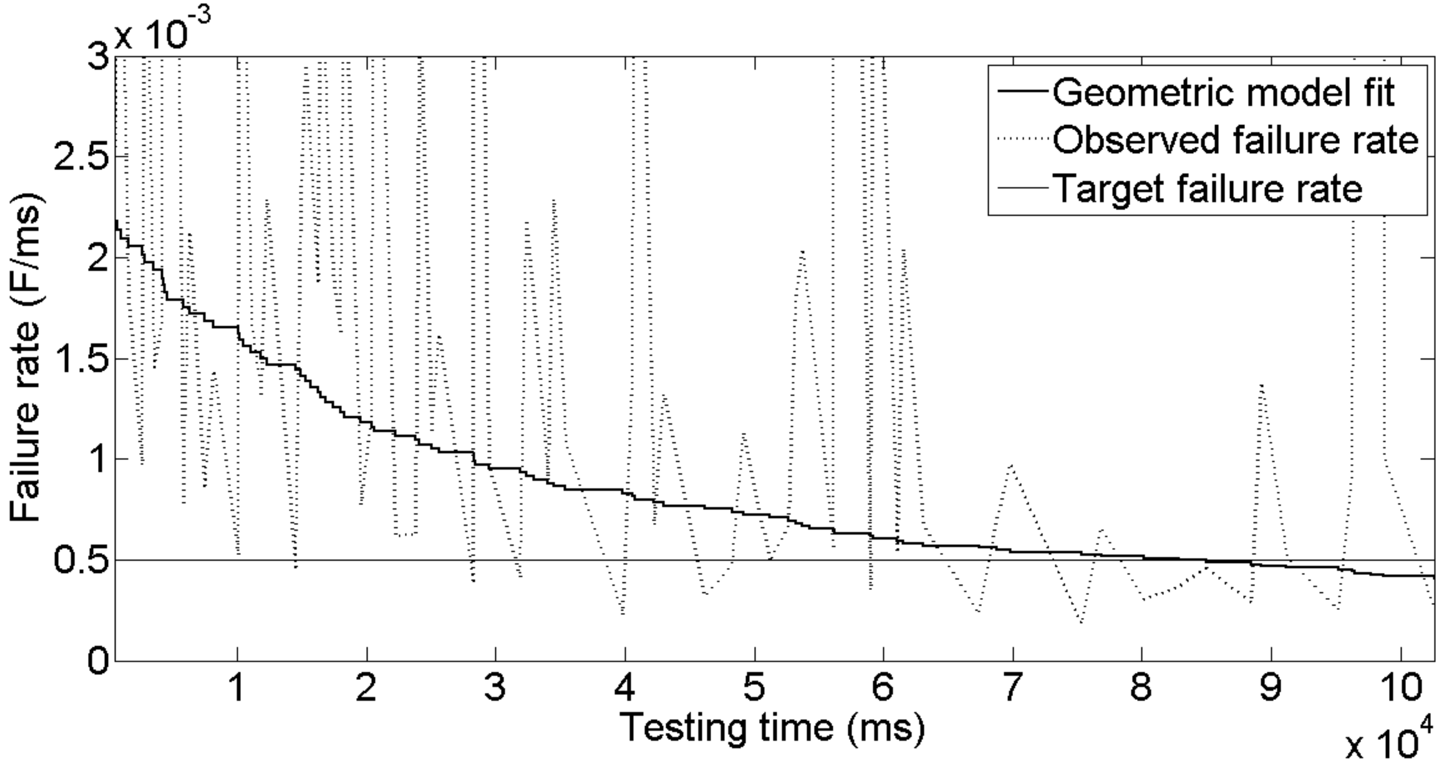
Summary of Year I deliverables

- Implemented open source software reliability tool
  - Data conversion routines
  - Trend tests for reliability growth
  - Two failure rate models
    - Assume failure rate decreases as faults detected and removed
  - Three failure count models
    - Count faults detected as function of time
  - Tested on dozens of data sets
  - Two goodness of fit measures

Estimates enabled by software reliability models

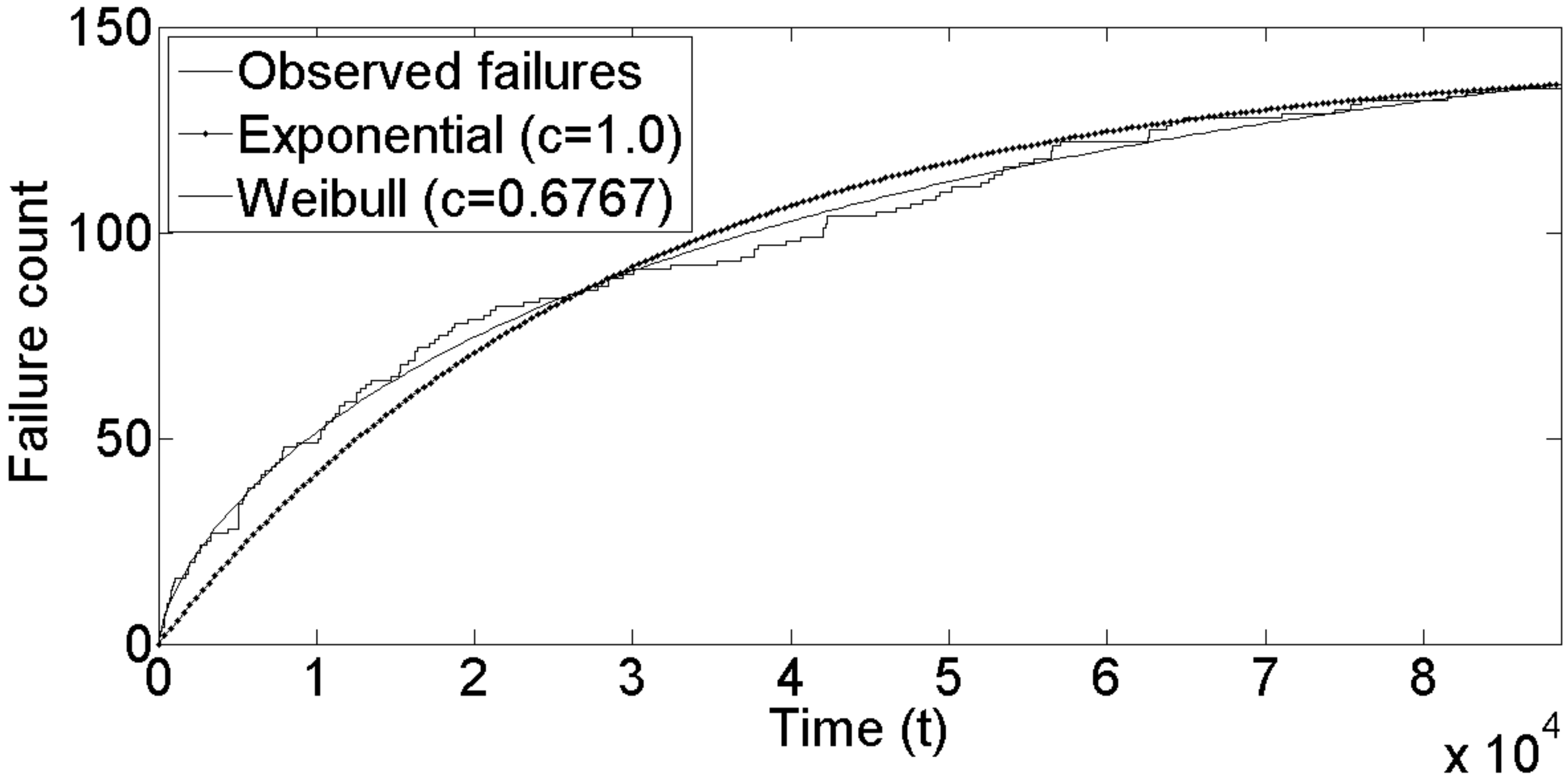
- Number of
  - Faults detected with additional testing
  - Remaining faults
- Mean time to failure (MTTF) of next fault
  - Testing time needed to remove next k faults
- Probability software does not fail before completion of fixed duration mission

Failure rate model



Model characterizes decreasing trend in failure rate

Failure time/count models



Model characterizes fault discovery process

UMass | Dartmouth UNIVERSITY OF MASSACHUSETTS DARTMOUTH

sasdlc.org/lab/projects/srt.html

Software Failure and Reliability Assessment Tool (SFRAT)

Description

The key to the success of all software is its reliability. The Software Failure and Reliability Assessment Tool (SFRAT) is an open source application to estimate and predict the reliability of a software system during test and operation. It allows users to answer the following questions about a software system during test:

1. Is the software ready to release (has it achieved a specified reliability goal)?
2. How much more time and test effort will be required to achieve a specified goal?
3. What will be the consequences to the system's operational reliability if not enough testing resources are available?

SFRAT runs under the R statistical programming framework and can be used on computers running Windows, Mac OS X, or Linux

Resources

WARNING: Web instance is for demonstration only. Please do not upload sensitive data to the site

Web instance
Example failure data sets
SFRAT Github repository
User's Guide
Contributor's Guide

Publications

Search:

Year	Type	Publication

GUIDANCE

Software Reliability Growth Modeling

- No single model characterizes all data sets best
- Models supplementary mathematical guidepost
  - Used in conjunction with SDLC activities to identify, implement, and test functional requirements
- Do not prescribe a single model
- Learn to track before planning in SEPs & TEMPs
- Emphasize
  - Effective communication between system, reliability, and software engineers
  - Frequent use of quantitative SRGM throughout DT and OT to assess progress toward software and system reliability goals

Software Reliability Growth Tracking

- For reliability growth tracking to be effective
  - Failures and their severity must be clearly defined
  - Impact on mission and end-to-end capability in order to produce data suitable for reliability growth tracking
  - Will be impacted by updates to interacting subsystems including hardware, mechanical, sensing, and operator usage

Data formats

- Based on data formats
  - Failure Rate models
    - Inter-failure times - time between $(i-1)^{st}$ and i^{th} failure, defined as $t_i = (\mathbf{T}_i - \mathbf{T}_{i-1})$
    - Failure times – vector of failure times,

$$\mathbf{T} =< t_1, t_2, \dots, t_n >$$

  - Failure Counting models
    - Failure count data - length of the interval and number failures observed within it,

$$< \mathbf{T}, \mathbf{K} >=< (t_1, k_1), (t_2, k_2), \dots, (t_n, k_n) >$$

  - Possible to use change requests during DT

Data quality

- Accuracy
  - Critically depends on availability of failure data
  - Inaccurate records of time make model fitting and prediction difficult
- Even when data available
  - Practitioner must know how to filter and organize data for use in models
    - Filter to exclude: non-software issues, duplicate failures, etc…

SOFTWARE FAILURE AND RELIABILITY ASSESSMENT TOOL (SFRAT)

ARCHITECTURE

SFRAT user modes

- Graphical user interface
  - Web and intranet
- Developer mode
  - Incorporate additional models
- Power user
  - Incorporate into internal software testing processes
- Benefits
  - Can help contractors, FFRDCs, and government quantitatively assess software as part of data collection, reporting, and oversight

SFRAT – File structure

install_script.R

server.R

ui.R

utility

- Data
  - a.Data_Tools.R
- Metrics
  - a.GOF.R
- Plots
  - a.PlotModelResults.R
  - b.Plot_Raw_Data.R
  - c.Plot_Trend_Tests.R
- Prediction
  - a.Detailed_prediction.R
- tables
  - a.DataAndTrendTables.R
  - b.ModelResultTable.R
- RunModels.R

trend_tests

1. Laplace_trend_test.R
2. RAA.R

models

- GO
- DSS
- Wei
- JM
- GM

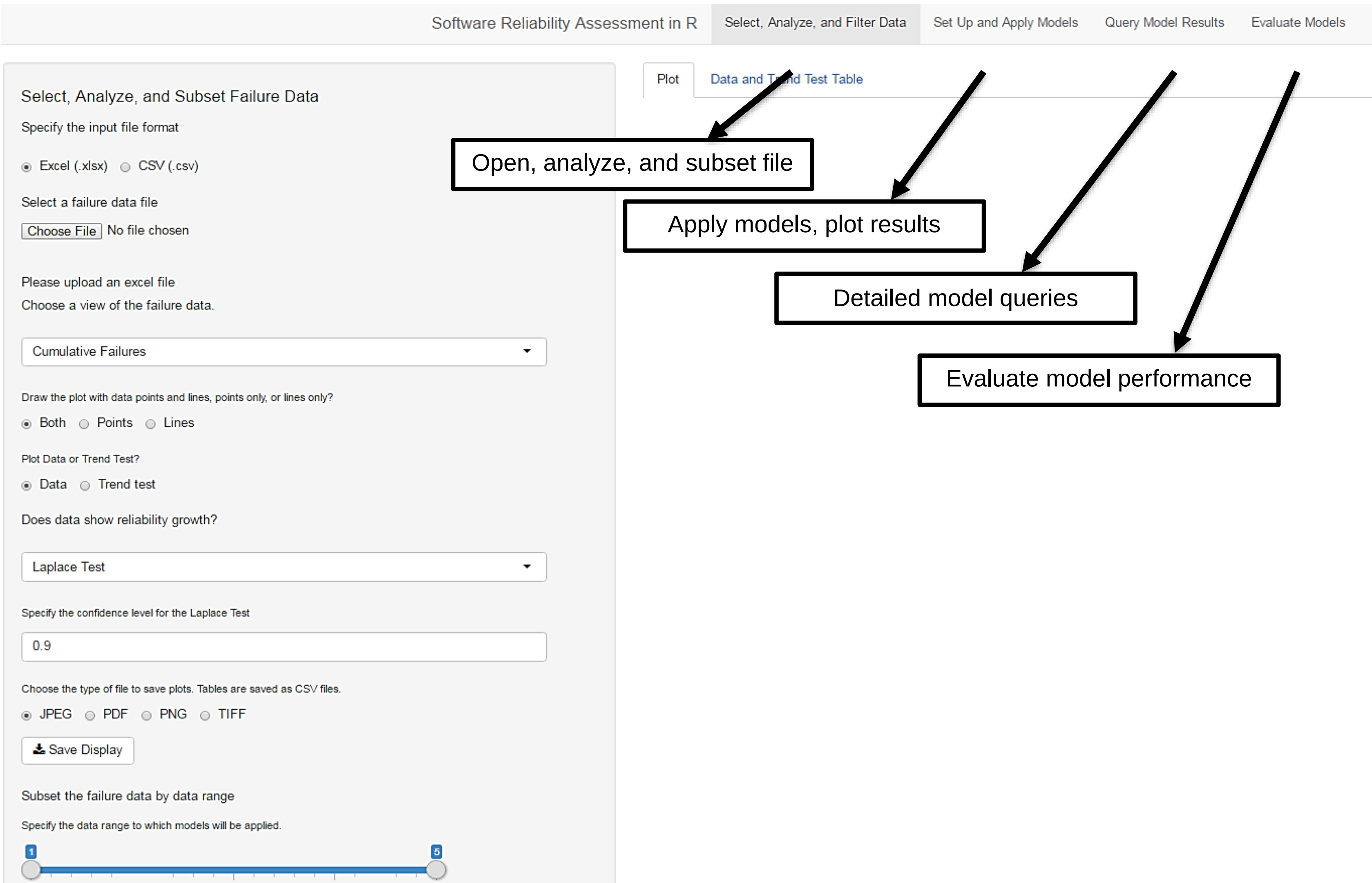
New models added in the “models” folder

Power user mode

- Code can be tailored for internal use
  - Build into existing automated software testing procedures to provide near real-time feedback of reliability trends
  - Many industry standard programming languages can call R functions
    - Visual Basic, Java, C/C#/C++, and Fortran
    - Ensures tool will integrate smoothly

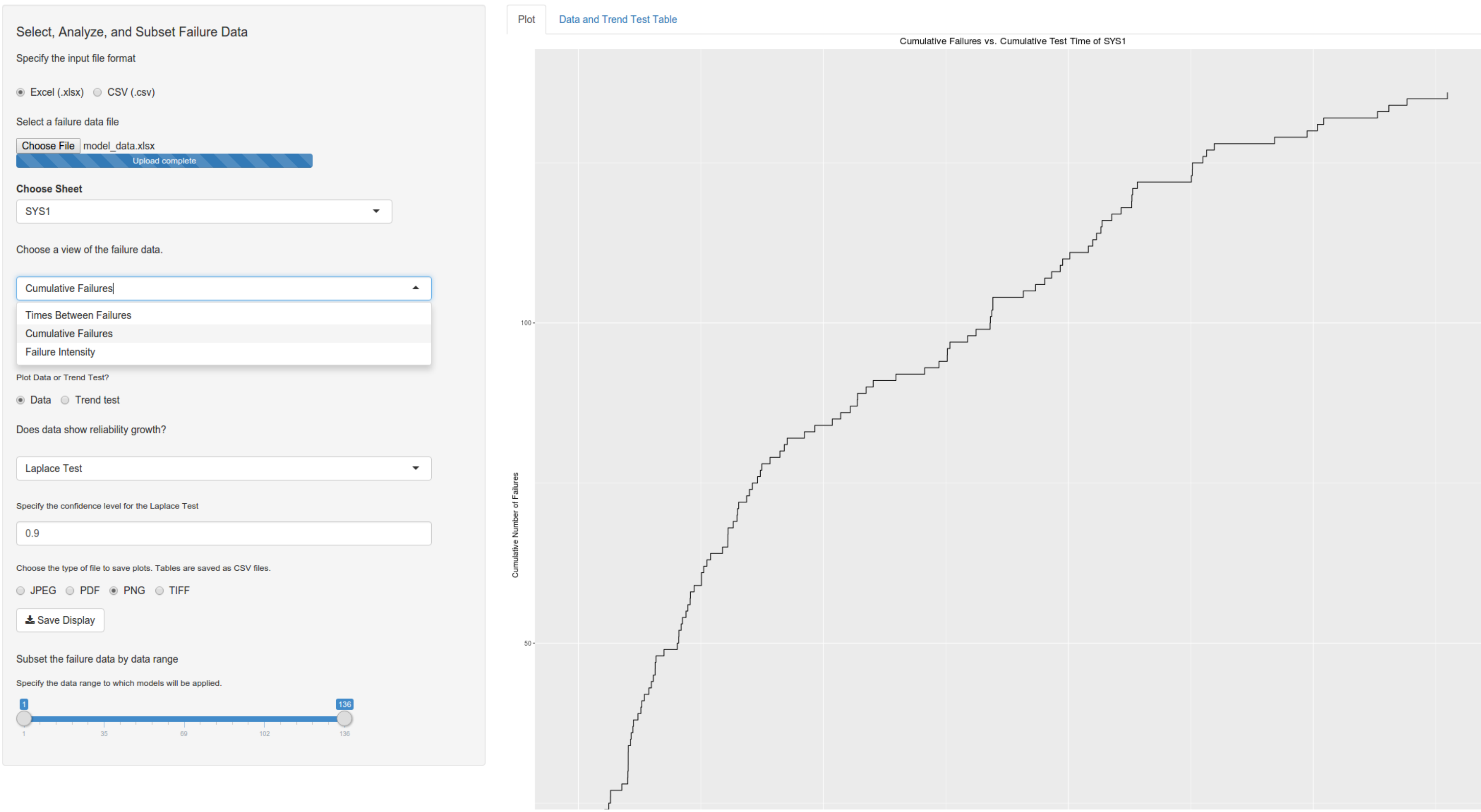
REVIEW OF YEAR I FUNCTIONALITY

SFRAT - Tab view



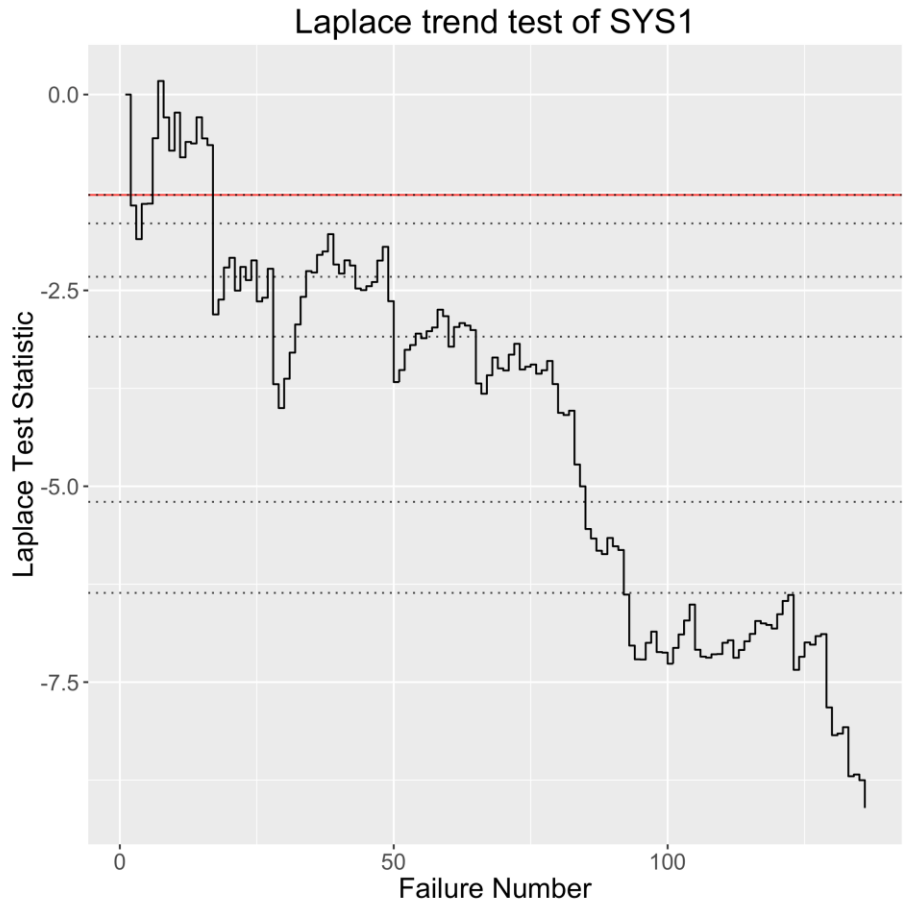
Tab 1
Select, Analyze, and Filter data

Tab 1 – After data upload



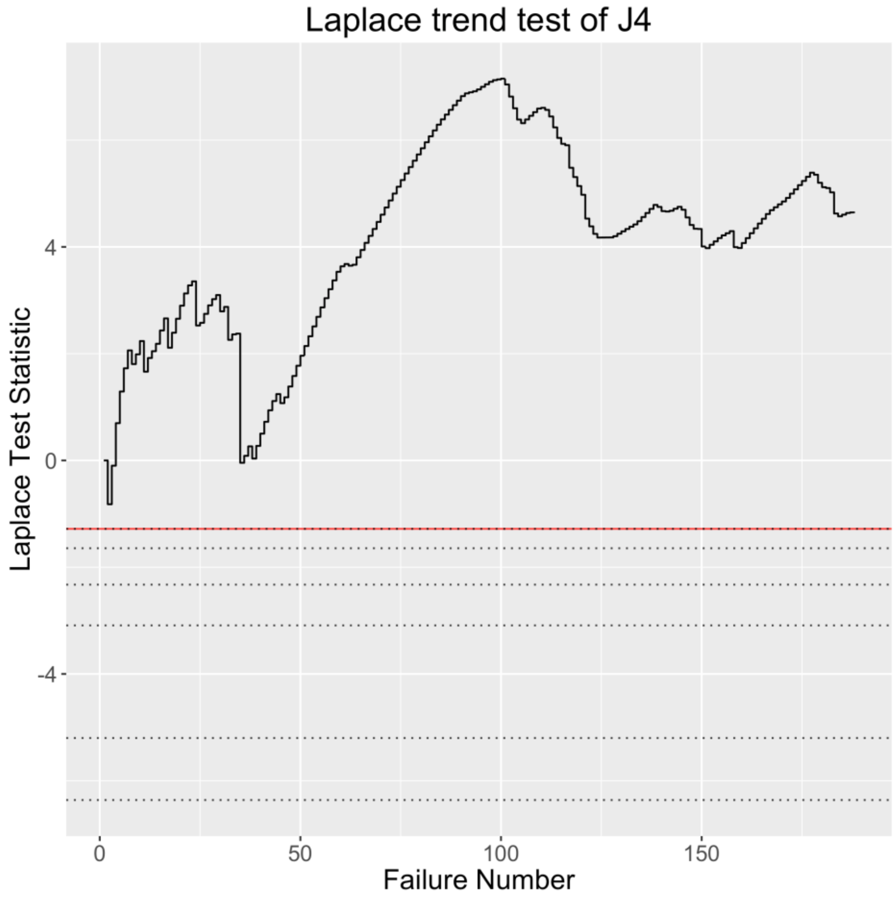
Cumulative failure data view

Laplace trend test – SYS1 data



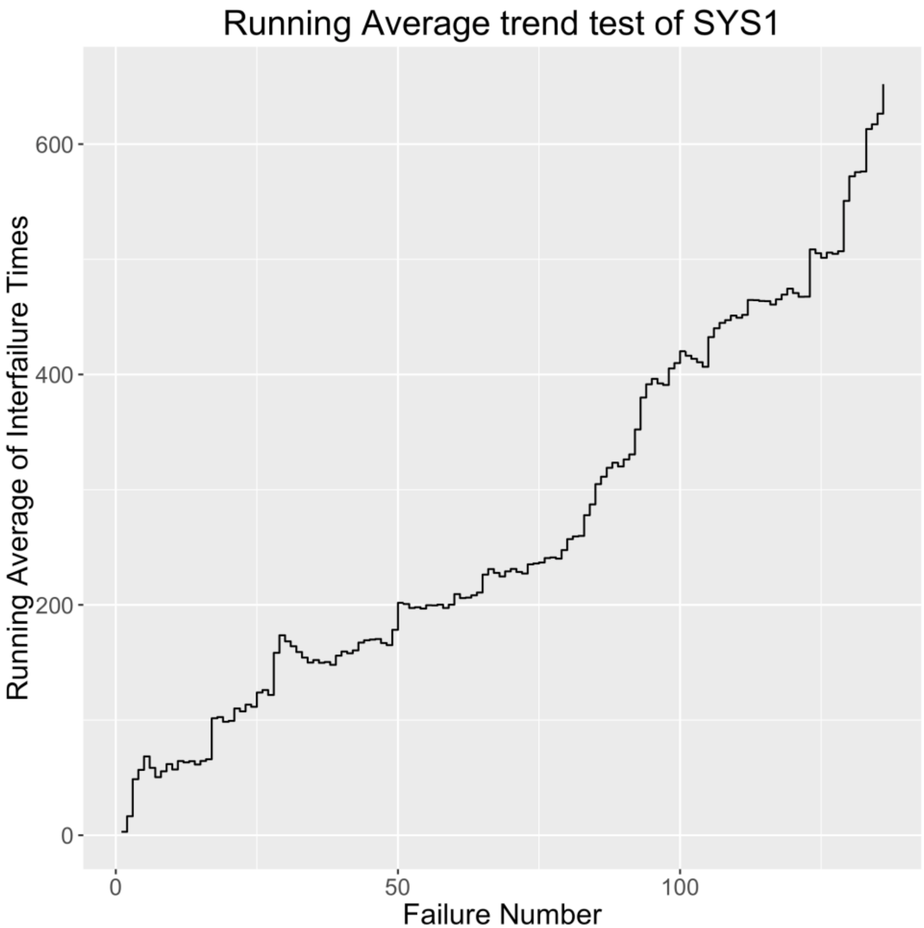
Decreasing trend indicates reliability growth
(Indicates application of SRGM appropriate)

Laplace trend test – J4 data



Does not exhibit reliability growth
(Indicates additional testing required)

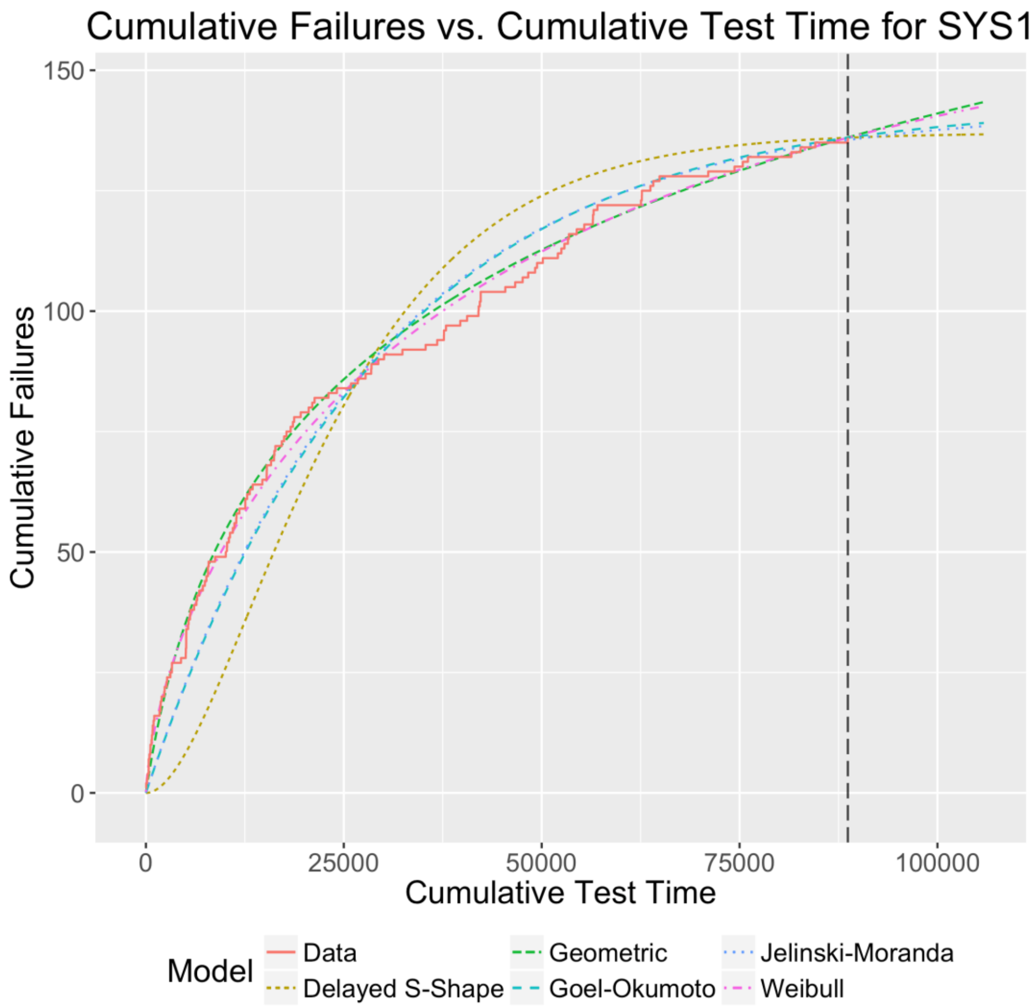
Running Arithmetic Average – SYS1 data



Increasing trend indicates reliability growth

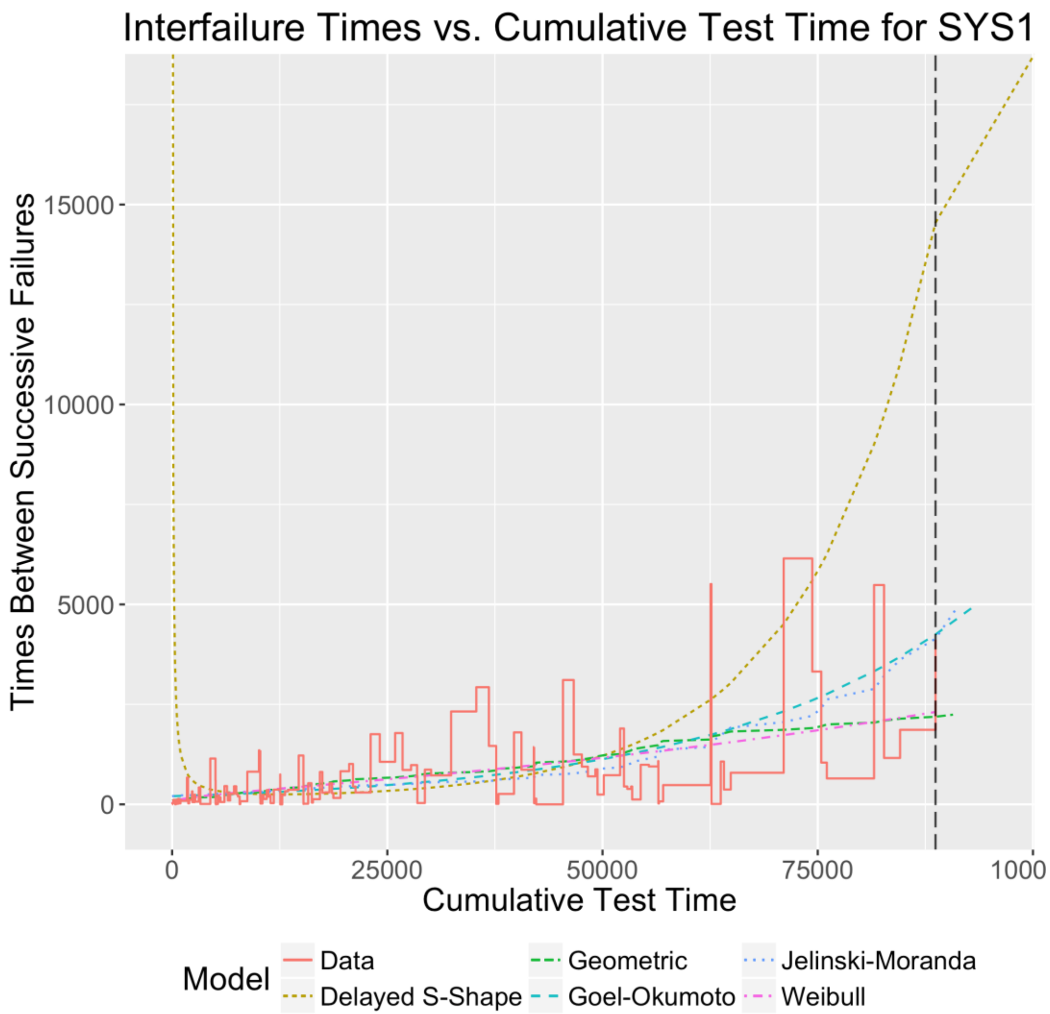
Tab 2
Set Up and Apply Models

Cumulative failures



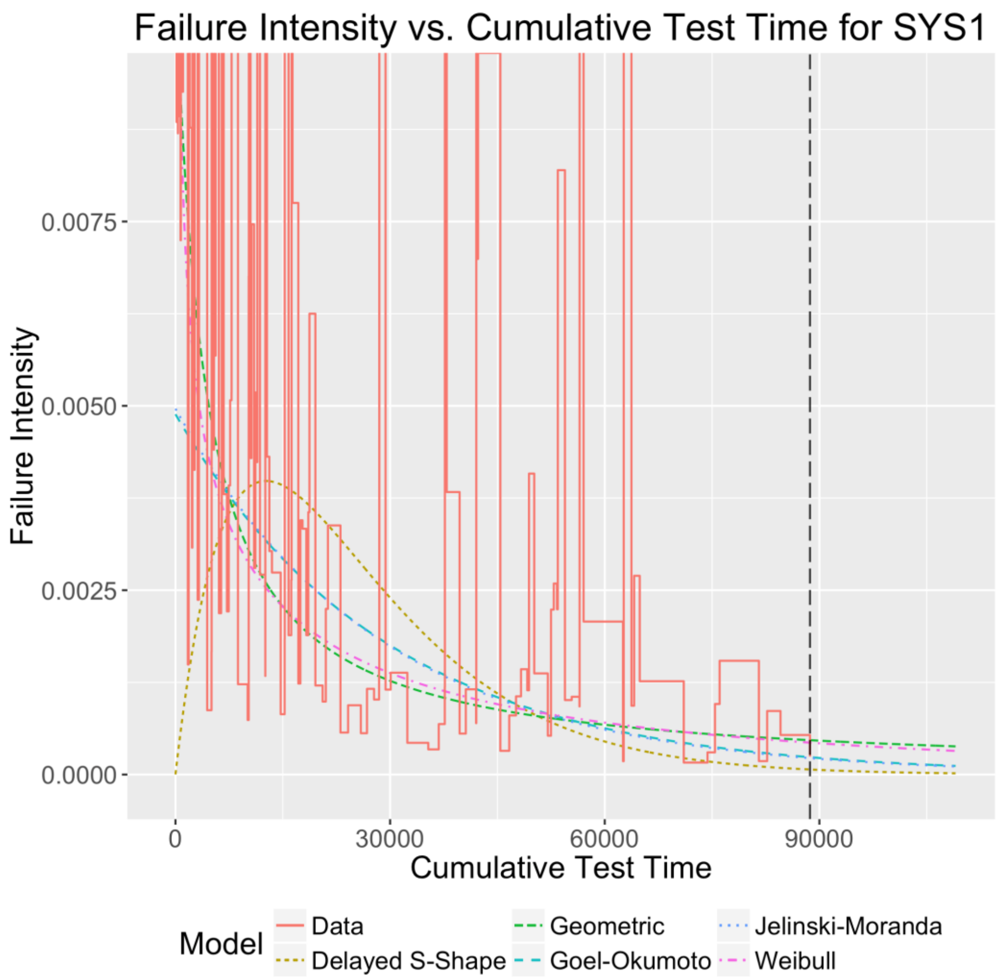
Plot enables comparison of data and model fits

Time between failures



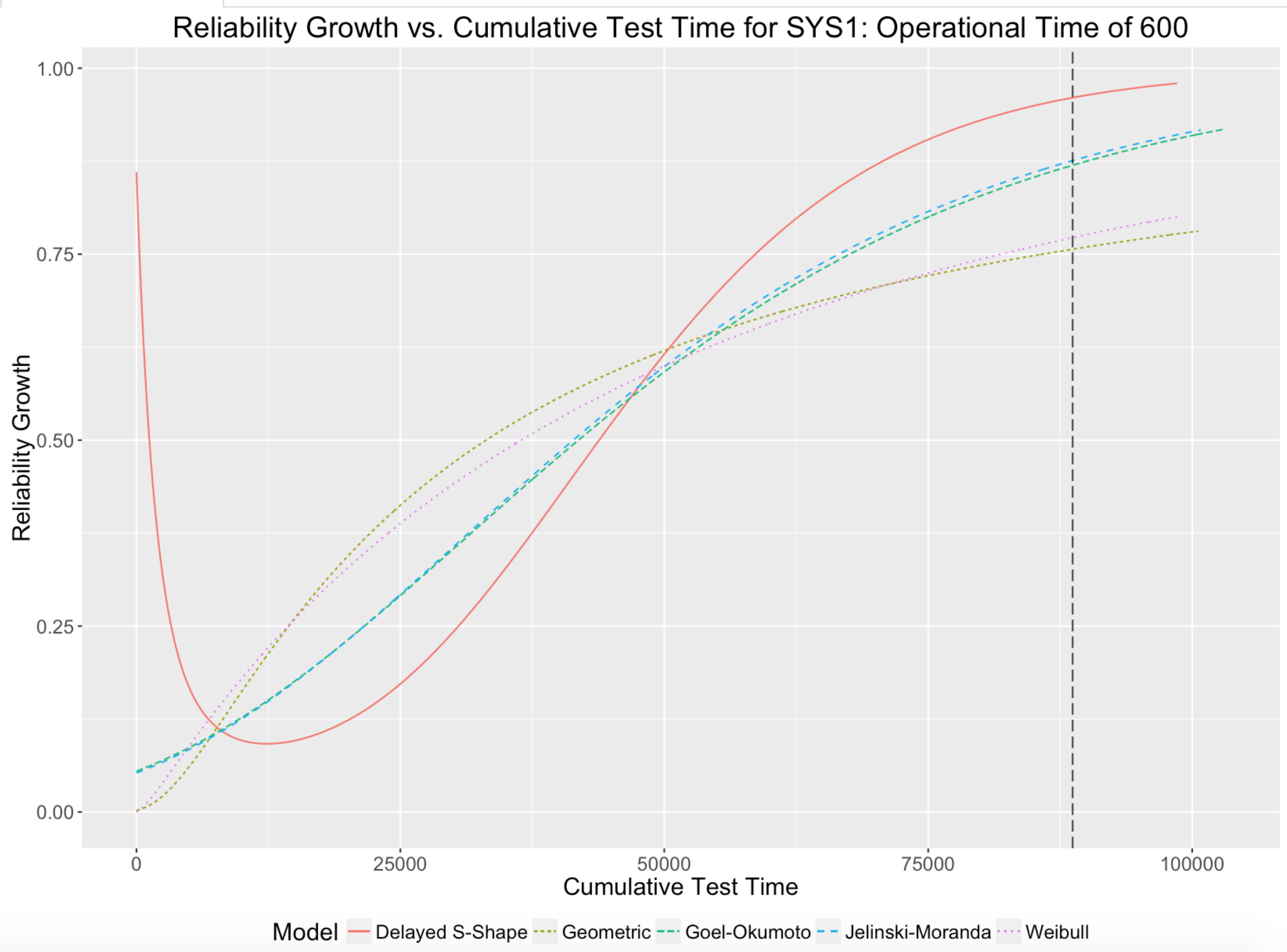
Times between failures should increase (indicates reliability growth)

Failure intensity



Failure intensity should decrease (indicates reliability growth)

Reliability growth curve



Can determine time to achieve target reliability

Tab 3
Query Model Results

Failure Predictions

	Model	Time to achieve R = 0.9 for mission of length 4116	Expected # of failures for next 4116 time units	Nth failure	Expected times to next 1 failures
	All	All	All	All	All
1	Delayed S-Shape	12401.1541529981	0.2468563	1	NA
2	Geometric	1592716.45936287	1.8774731	1	2170.03088926781
3	Goel-Okumoto	62829.7672027733	0.9036154	1	4591.28466949961
4	Jelinski-Moranda	59915.2917457156	0.8561255	1	4869.80650205625
5	Weibull	259865.770847692	1.7259537	1	2353.05254648438

Showing 1 to 5 of 5 entries

Previous 1 Next

Can identify potential schedule overruns

Tab 4
Evaluate Models

AIC and PSSE

	Model	AIC	PSSE
	All	All	All
1	Delayed S-Shape	2075.146	296.34925
2	Geometric	1937.034	84.32708
3	Goel-Okumoto	1953.613	23.07129
4	Jelinski-Moranda	1950.534	19.60037
5	Weibull	1938.161	74.94496

Showing 1 to 5 of 5 entries

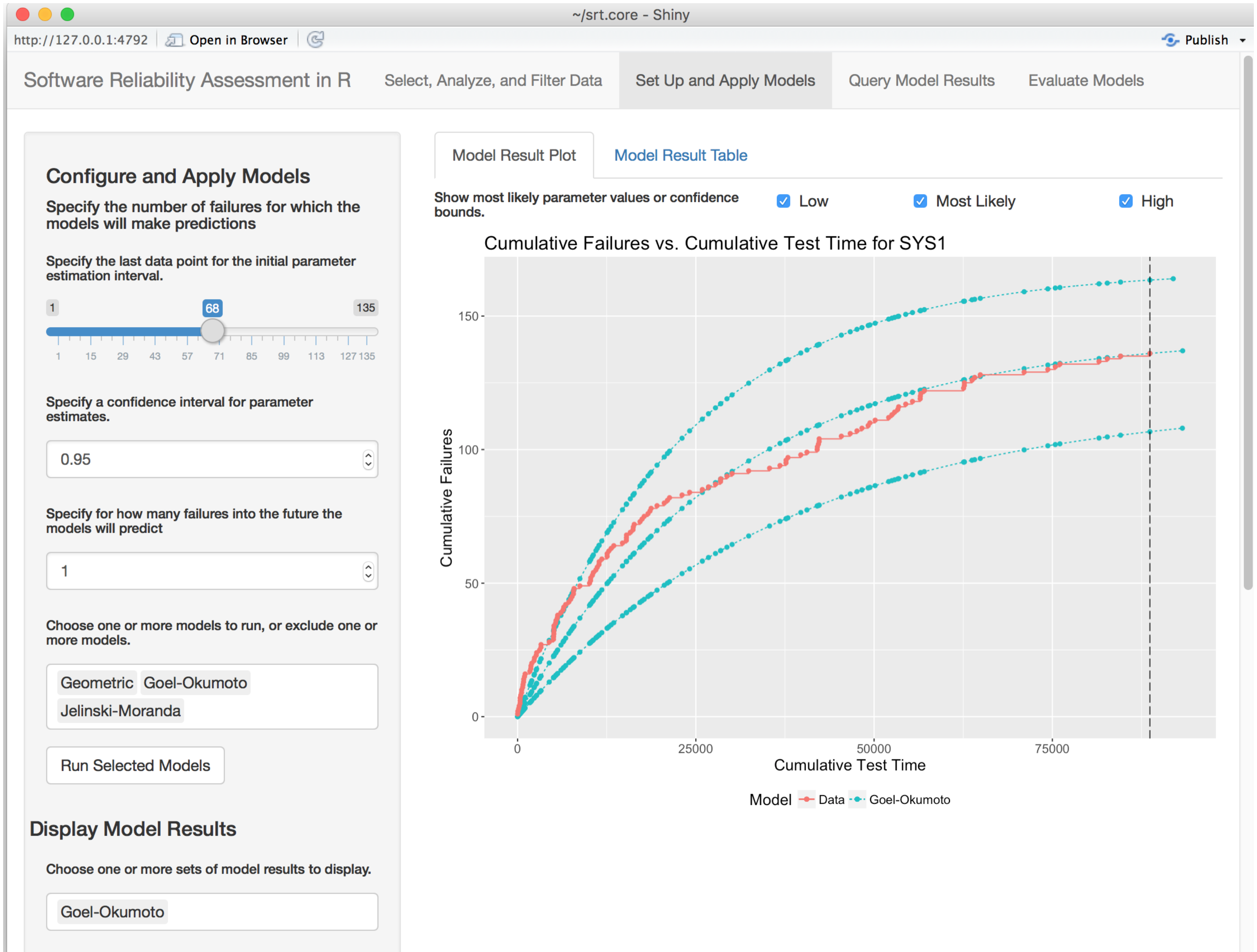
Previous 1 Next

Lower values preferred

YEAR II (7/16-7/17) SFRAT FUNCTIONALITY

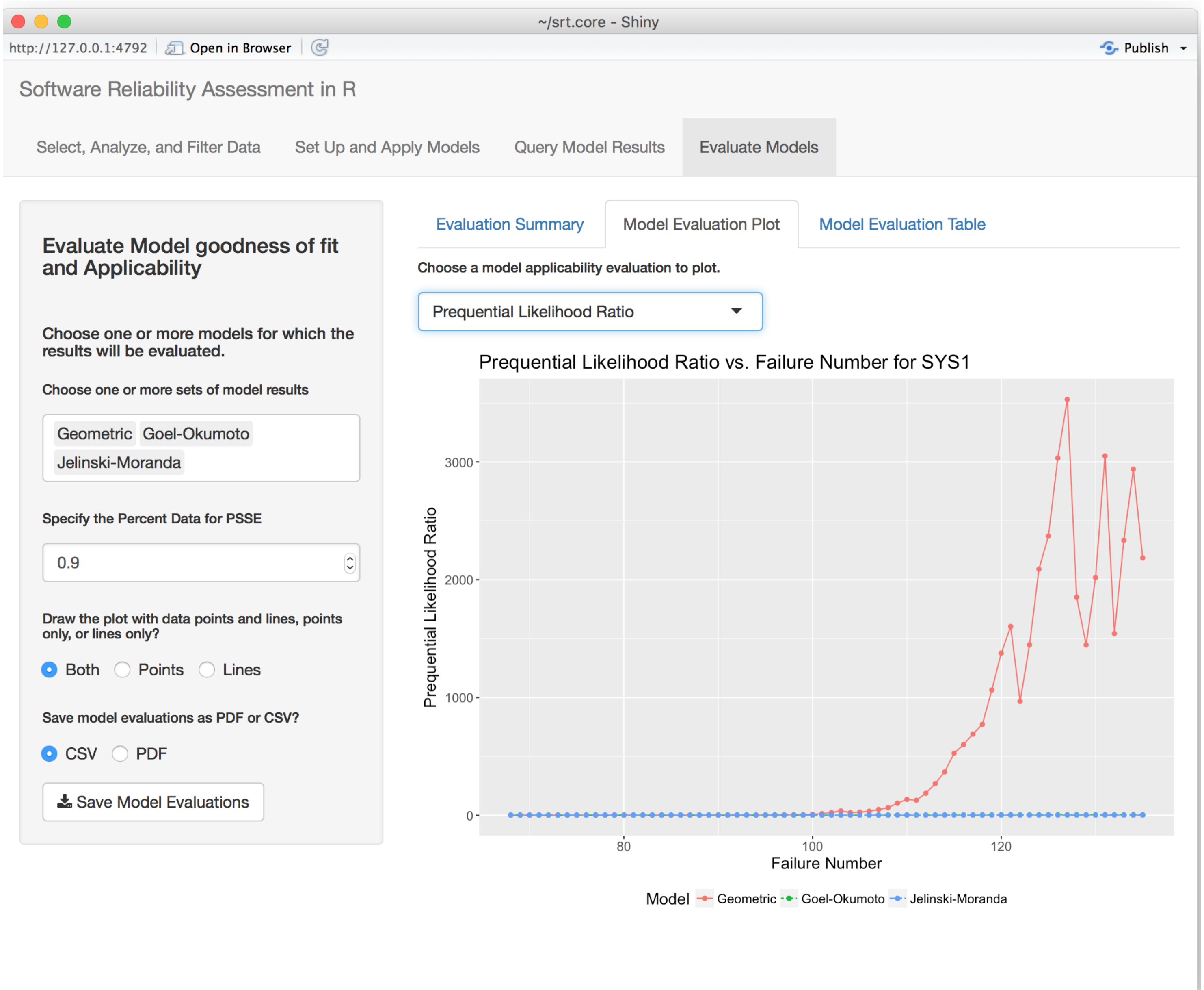
- Upper and lower confidence limits
  - Graphical and tabular values
- Model Evaluation Criteria
  - Prequential likelihood (PL) ratio
    - Identify model more likely to produce accurate estimates
      - Higher preferred
  - Model bias (MB) and MB trend
    - Indicate whether model over/underestimates times between failures
- Optimal release

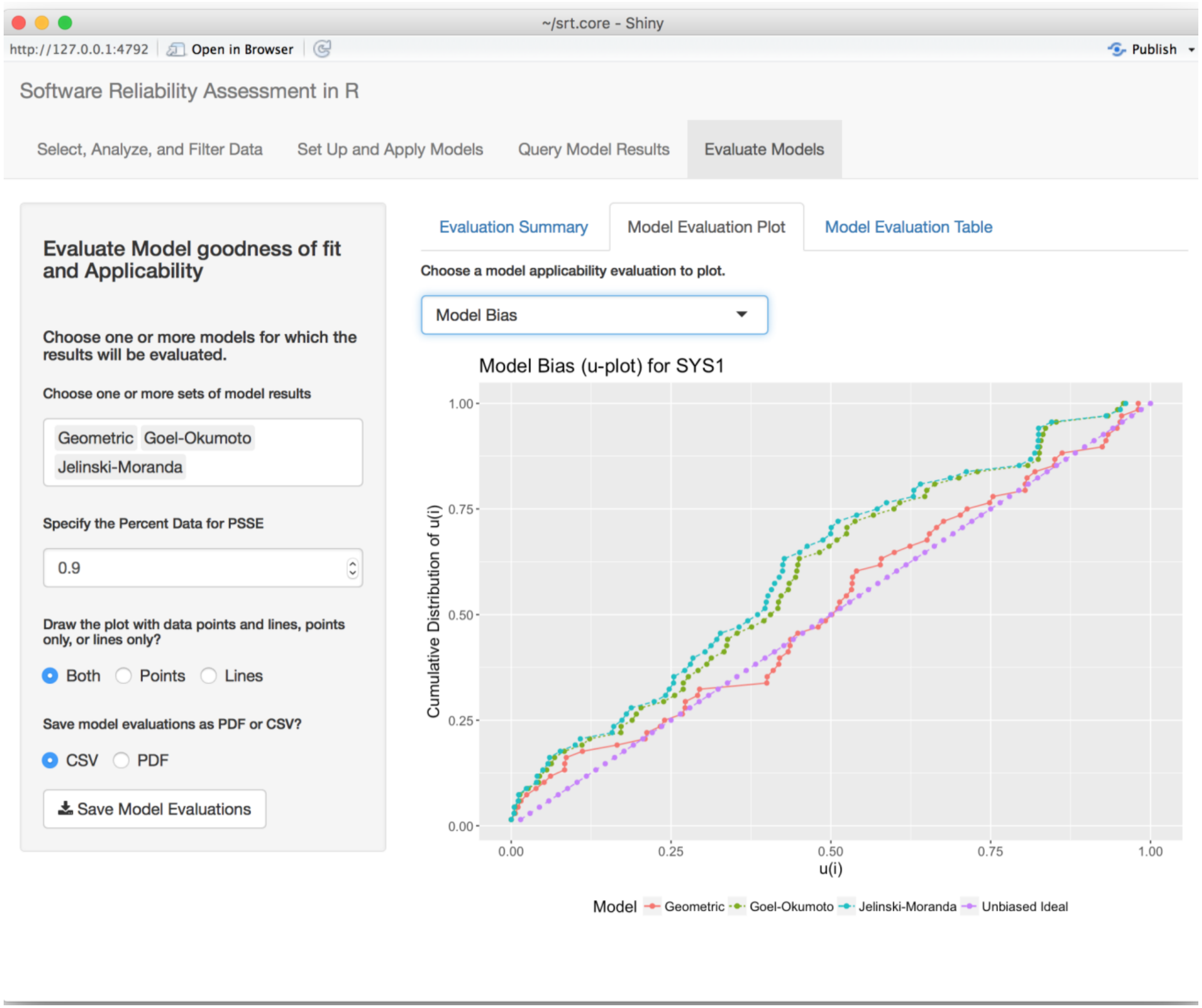
UMass | Dartmouth UNIVERSITY OF MASSACHUSETTS DARTMOUTH



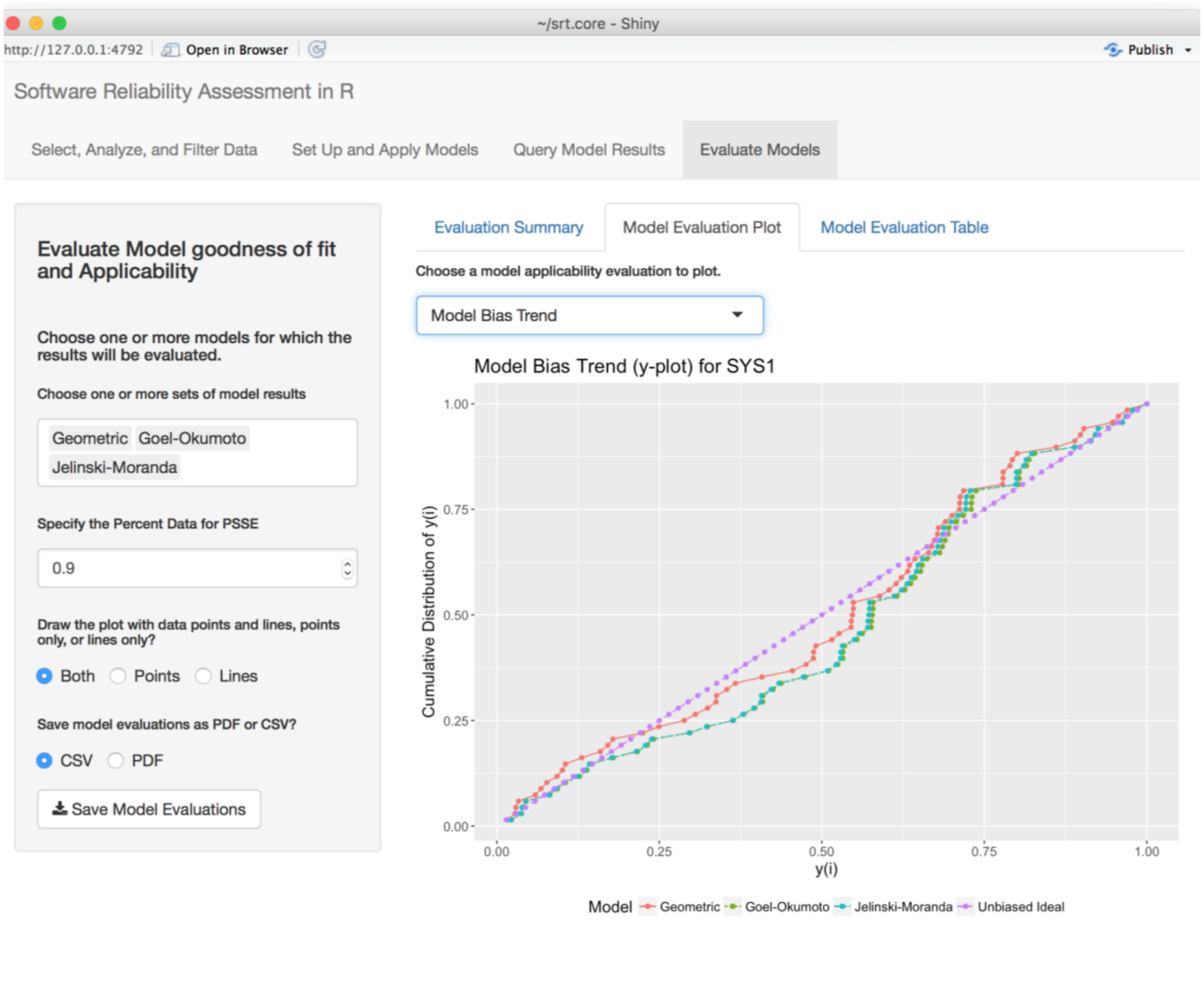
UMass | Dartmouth

UNIVERSITY OF MASSACHUSETTS DARTMOUTH

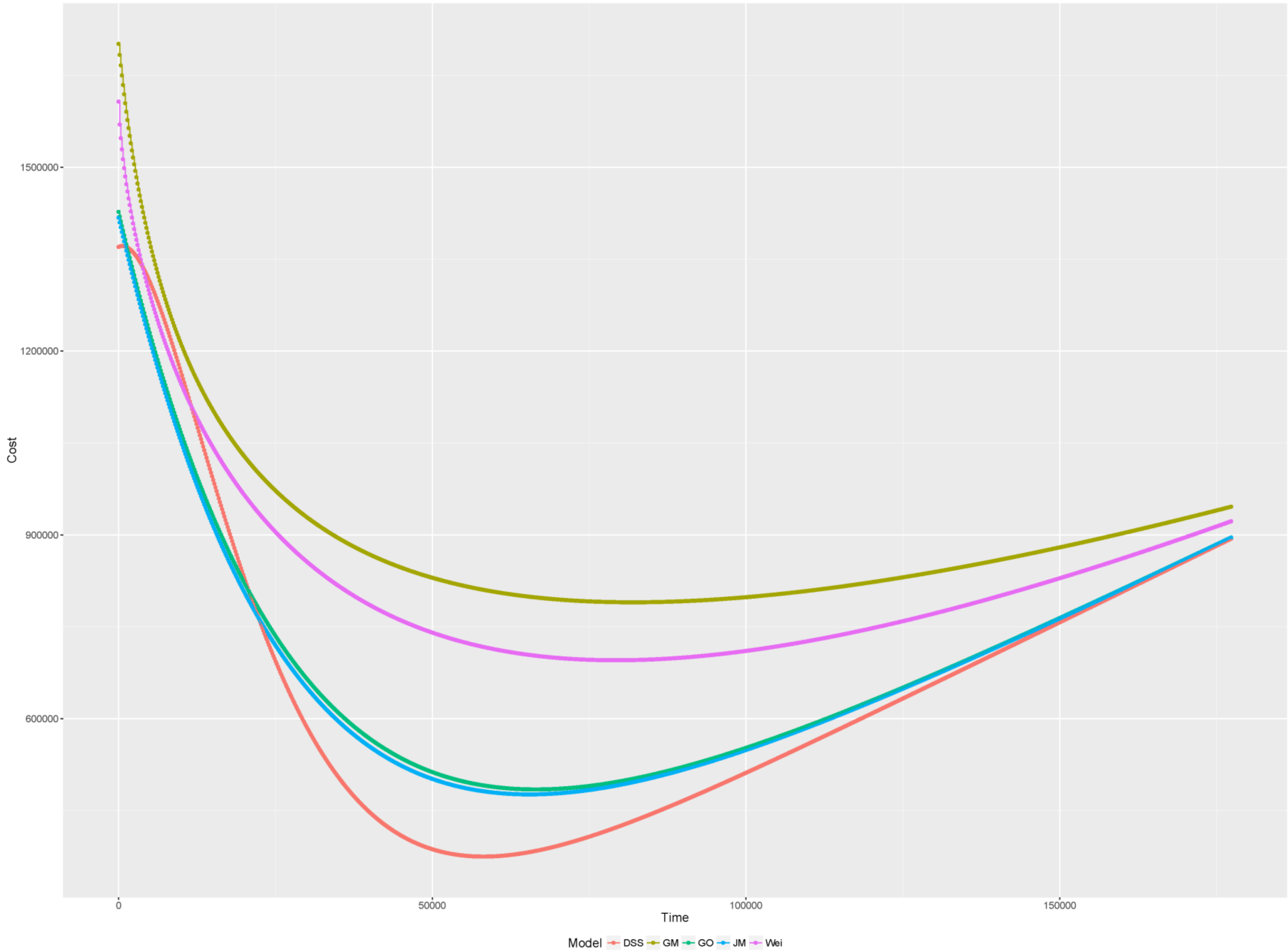




Models above line estimate more frequent times between failures than those observed



Models below line estimate more frequent times between failures than those observed


1500000
1200000
900000
600000
Cost
0
50000
100000
150000
Time
Model
DSS
GM
GO
JM
Wei

<u>S</u>OFT<u>W</u>ARE D<u>E</u>FECT <u>E</u>STIMATION <u>T</u>OOL (SWEET)

SWEEP (Software Error Estimation Program)

- Implemented four modes

1. Time-based model
   - Estimates and tracks errors during system test and integration cycle
2. Phase-based model
   - Provides defect information before running any code
3. Planning aid
   - Generates an error discovery profile based on historical data
4. Defect injection model
   - Allows user to understand probable defect injection profile

Software Defect Estimation Tool (SweET)

Description

The Software Defect Estimation Tool (SweET) is an open source application to track error identification and removal efforts during the software development lifecycle. SwEET is a free and open source version of the SoftWare Error Estimation Program (SWEEP) and SweET uses Weibull software reliability growth model utilizing Expectation Conditional Maximization algorithm to ensure stability and performance of the model fitting process. SweET simplifies four models of SWEEP into three modes:

1. **Mode A**: Time-based model: Estimates and tracks errors during system test and integration cycles.
2. **Mode B**: Phase-based and planning aid model: Predict and track defects for multiple phases and can provide defect information before running any code, whereas the planning aid model generates an error discovery profile based on the phase based historical data to help a software prohect achieve its objectives.
3. **Mode C**: Defect injection model: Allows the user to understand the probable defect injection profile and resulting efficiency and effectiveness of the verification process.

SweET runs under the Python 3.x programming framework and can be used on computers running Windows, Mac OS X, or Linux

Resources

Example data sets
SweET Github repository
User's Guide (In preparation)

GOALS

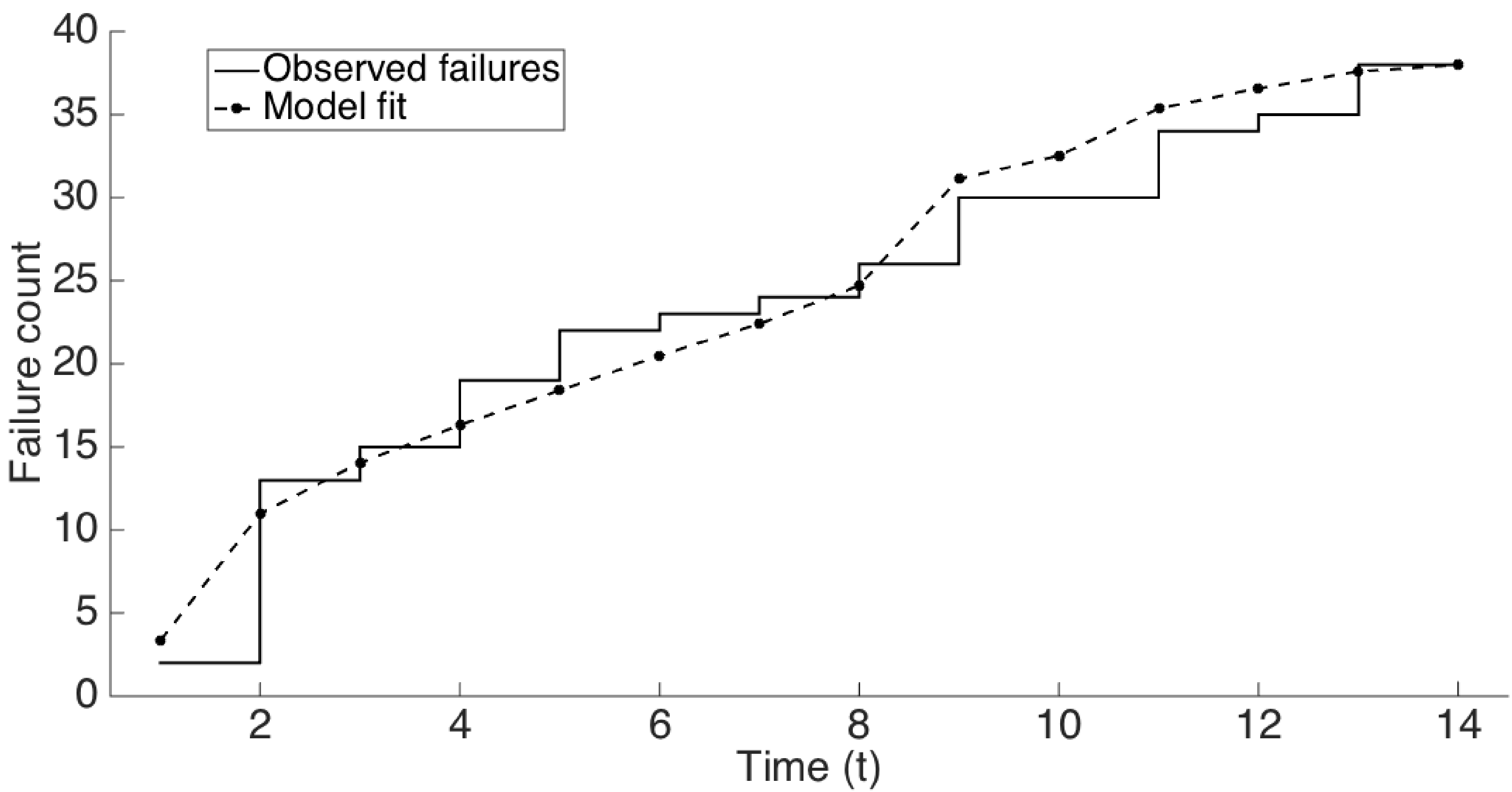
Activities

- Update documentation
- Outreach, education, and training
  - Visit DoD labs and listen to practical concerns underlying modeling requirements
  - Work with existing users
- Coordinate contributions from developers
  - Failure severity decomposition
  - Software readiness metrics
  - Additional models, Bayesian, covariate
  - Expand architecture to additional stages of lifecycle

Covariate data example

week	Execution Time (hr)	Failure Identification Work (person hr)	Computer Time-Failure Ident. (hr)	Failure Identified
1	.0531	4	1.0	1
2	.0619	20	0	1
3	.1580	1	0.5	2
4	.0810	1	0.5	1
5	1.0460	32	2.0	8
6	1.7500	32	5.0	9
7	2.9600	24	4.5	6
8	4.9700	24	2.5	7
9	0.4200	24	4.0	4
10	4.7000	30	2.0	3
11	0.9000	0	0	0
12	1.5000	8	4.0	4
13	2.0000	8	6.0	1
14	1.2000	12	4.0	0
15	1.2000	20	6.0	2
16	2.2000	32	10.0	2
17	7.6000	24	8.0	3
total	32.8000	296	60.0	54

Covariate model data fit



Stakeholder outreach

Acknowledgements

- This work was supported by (i) the Naval Air Warfare Center (NAVAIR) under contract N00421-16-T-0373 and (ii) the National Science Foundation (NSF) (#1526128).

Outpacing the Competition: A Systems Engineering Challenge

24 October 2017

Presented To:

NDIA Systems Engineering Conference

Presented By:

VADM Paul Grosklags, Commander, NAVAIR

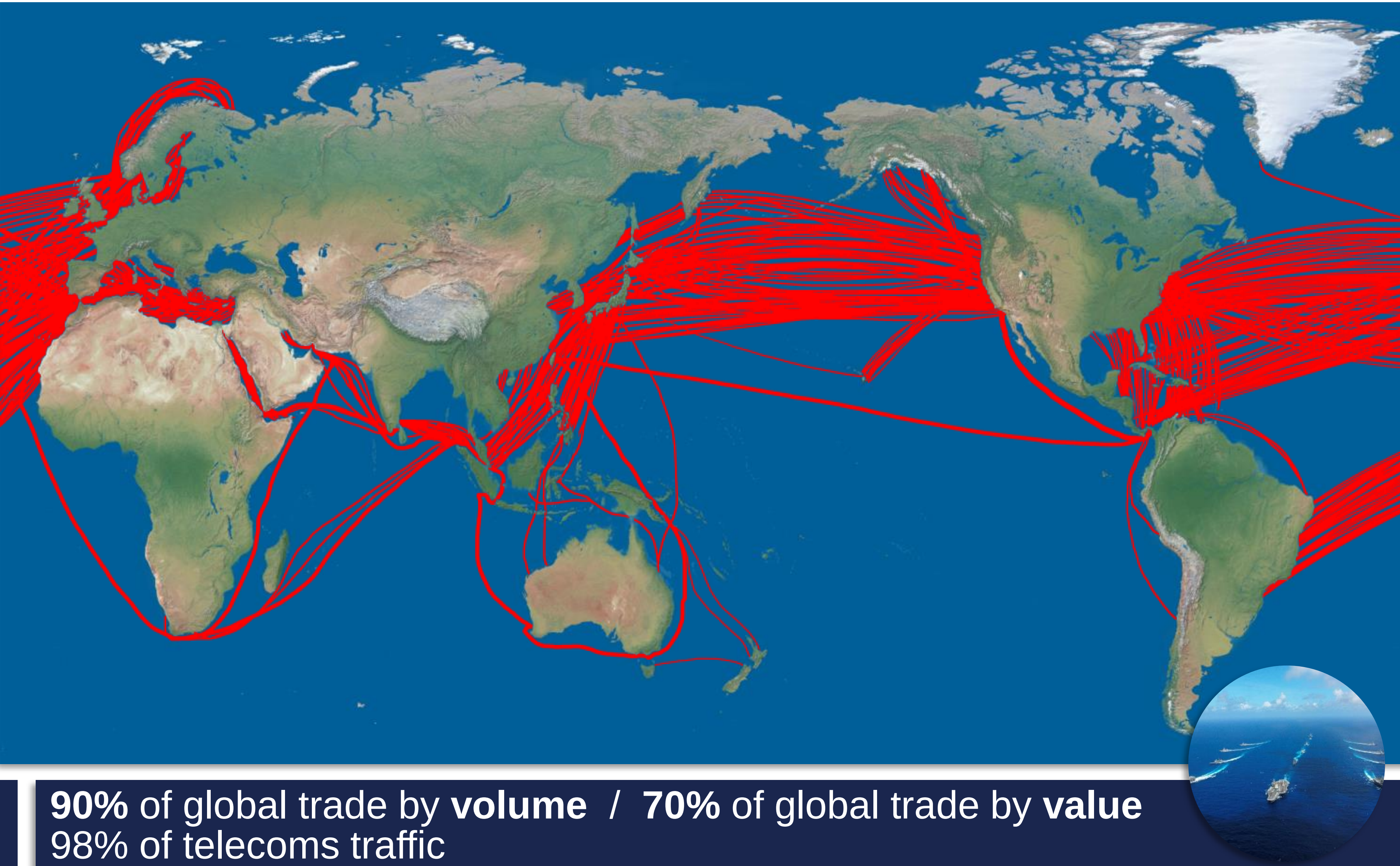
NAVAL AIR SYSTEMS COMMAND

Day in the life of an SE dealing with PMs

Framing the Challenge

Life Has Been Good!

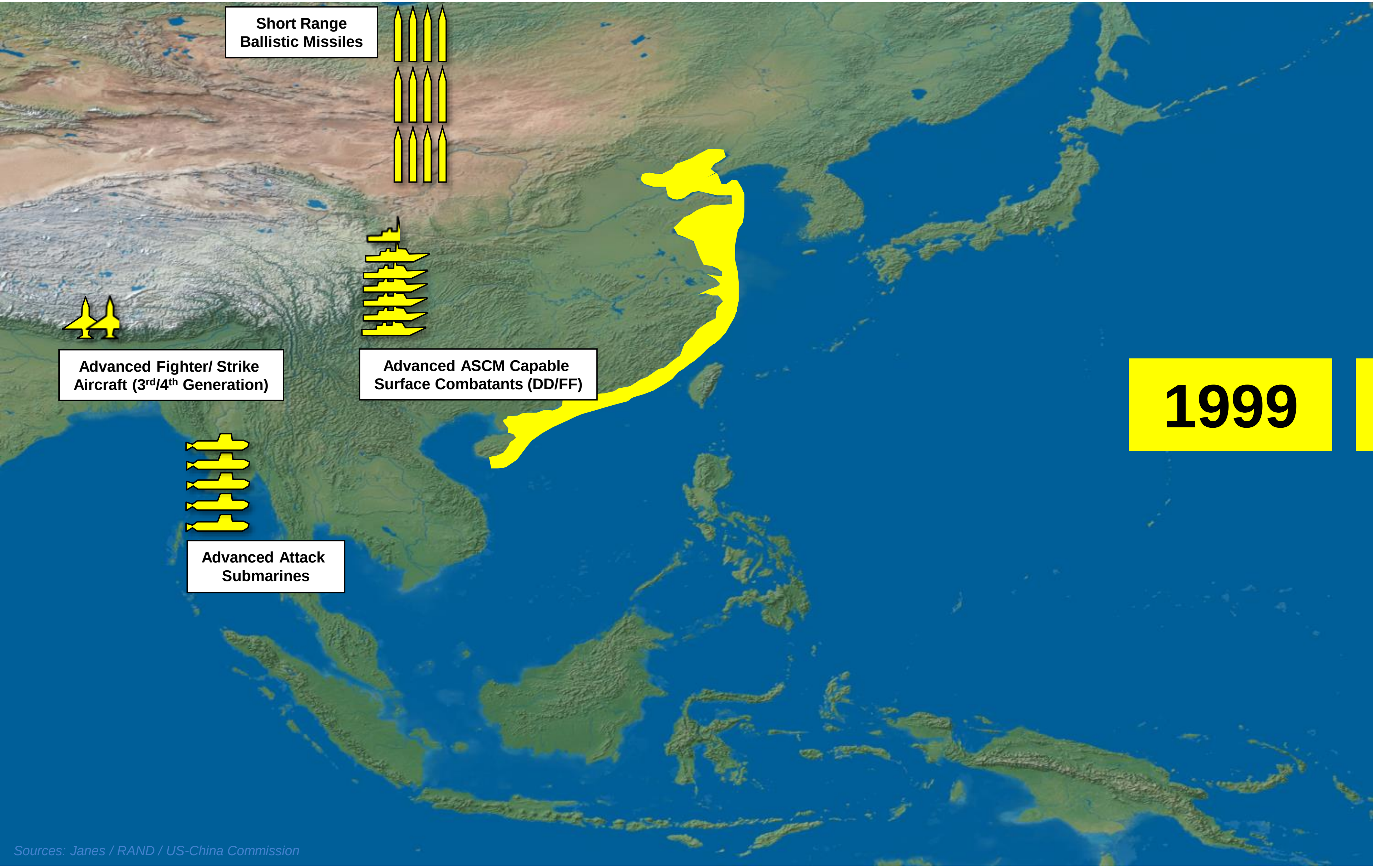
Sea Lanes Remain the Lifeblood of Our Economy



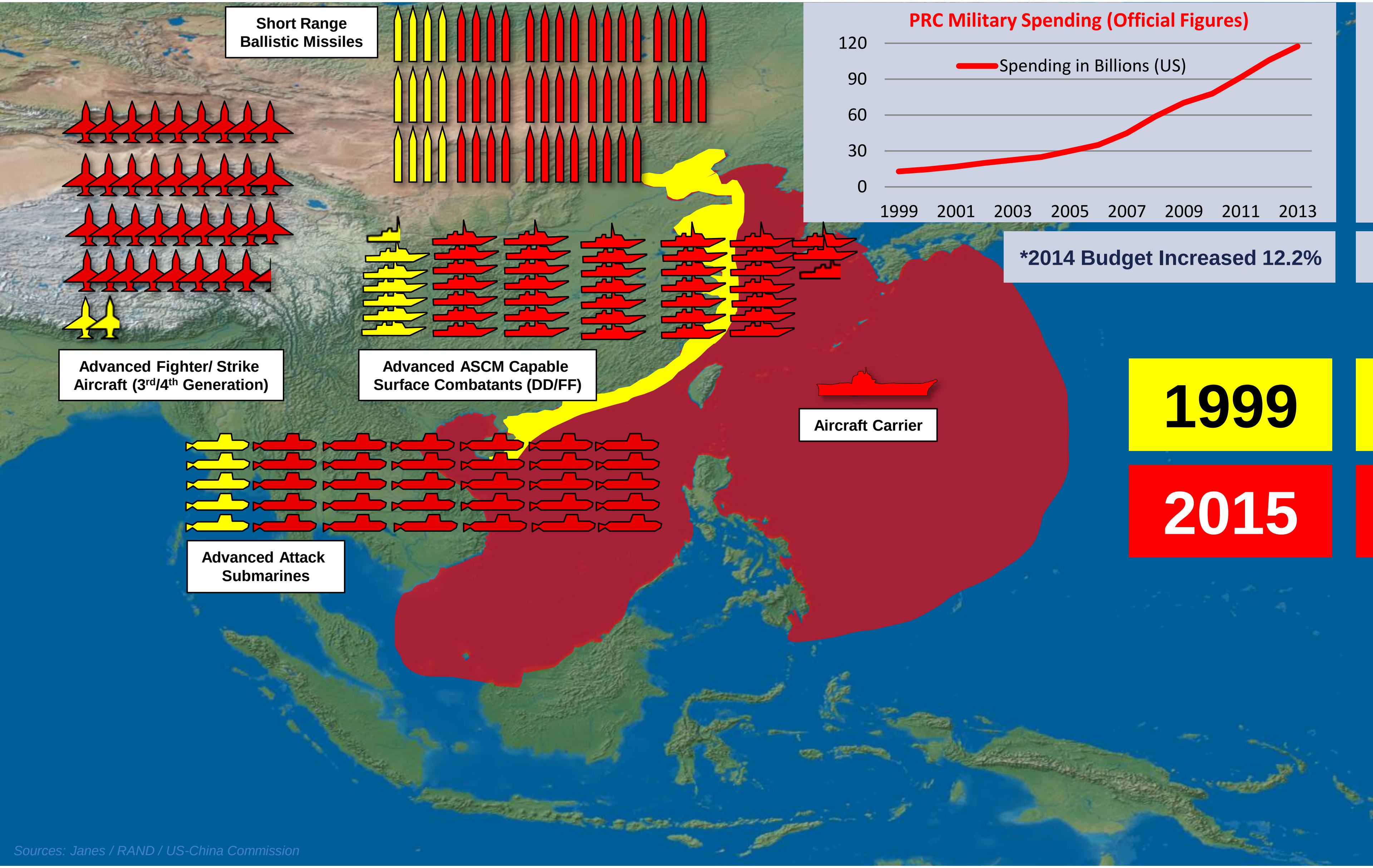
90% of global trade by **volume** / **70%** of global trade by **value**
98% of telecoms traffic

Competition is Back

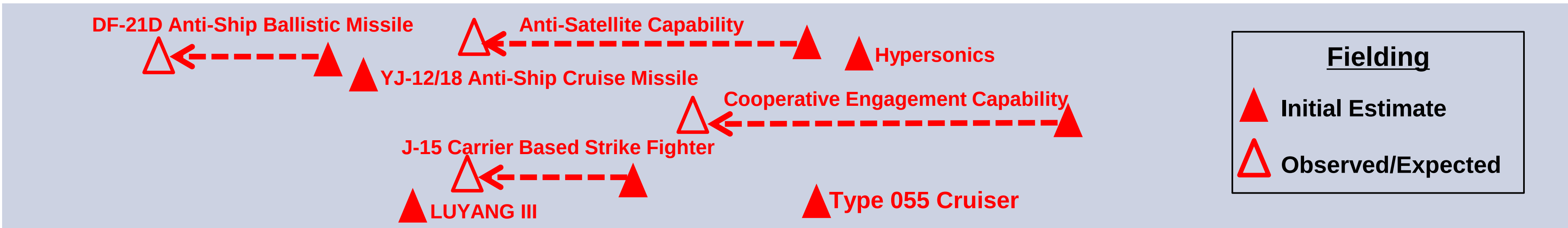
Changing Environment



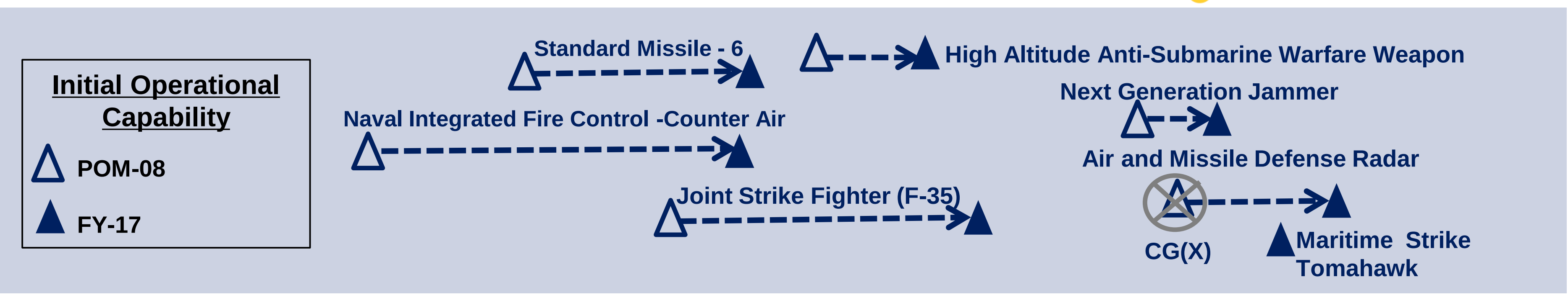
Changing Environment



USN and PLA(N) Capability Fielding Trends



We're Slower!



USN Warfighting Advantage has Steadily Eroded

CNO's Challenges to all Flag/SES

5 Key Points

Must be competitive → Existential Threat → No #2

Think Strategically → Critical Thinking

Going Digital

Outcome / Product Oriented → Vice Process

Sense of Urgency → Should be Uncomfortable

"If It's Not Making the Fleet More Lethal – Stop Doing It!"

NAVAIR Response

Commander's Intent – *Remains Unchanged*

- Increase Speed of New Capabilities to Fleet
- Increase Readiness

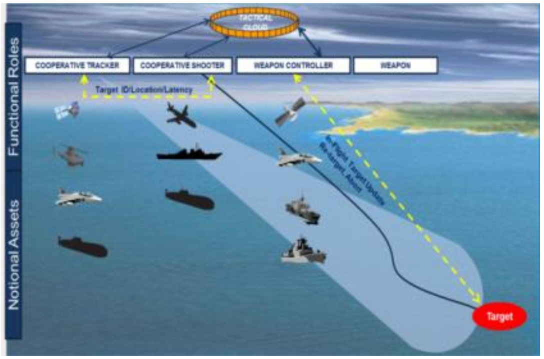
Strategic Initiatives – *Focus on Speed*

- Capabilities Based Acquisition – *Rapid delivery of integrated capabilities*
- Sustainment Vision 2020 – *Predictive, integrated sustainment operations*
- Digital Business Operations – *Integrated business systems "apps" at the desktop*

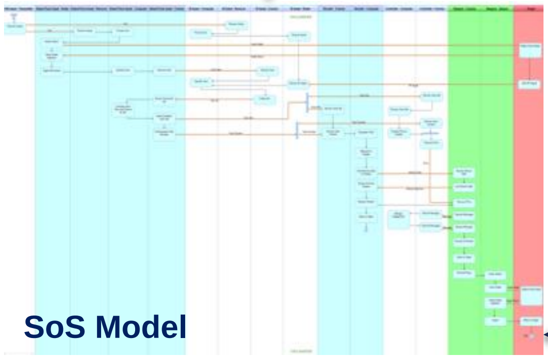
Accelerating delivery of fully integrated capabilities which are designed, developed, and sustained in a Model Based Digital Environment <u>IS</u> a Systems Engineering challenge

Capabilities Based Acquisition

Digital Thread Enables Rapid Delivery of Integrated Capabilities



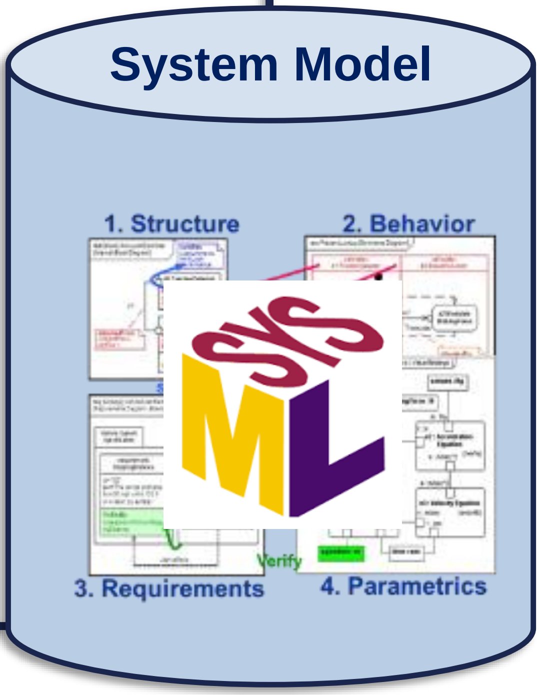
Integrated Warfare Analysis establishes CONEMPS, Effects-Chains, required attributes



CONEMPS and Effects Chains are modeled at the System of Systems (SoS) level

Digital Linkage

System models form “Constructive” basis for LVC M&S environment



Systems are developed in a Model-Based environment (SE Transformation)

Enabling Capabilities-Based T&E

Constructive	Virtual	Live

DIGITAL MODELING

HARDWARE IN THE LOOP

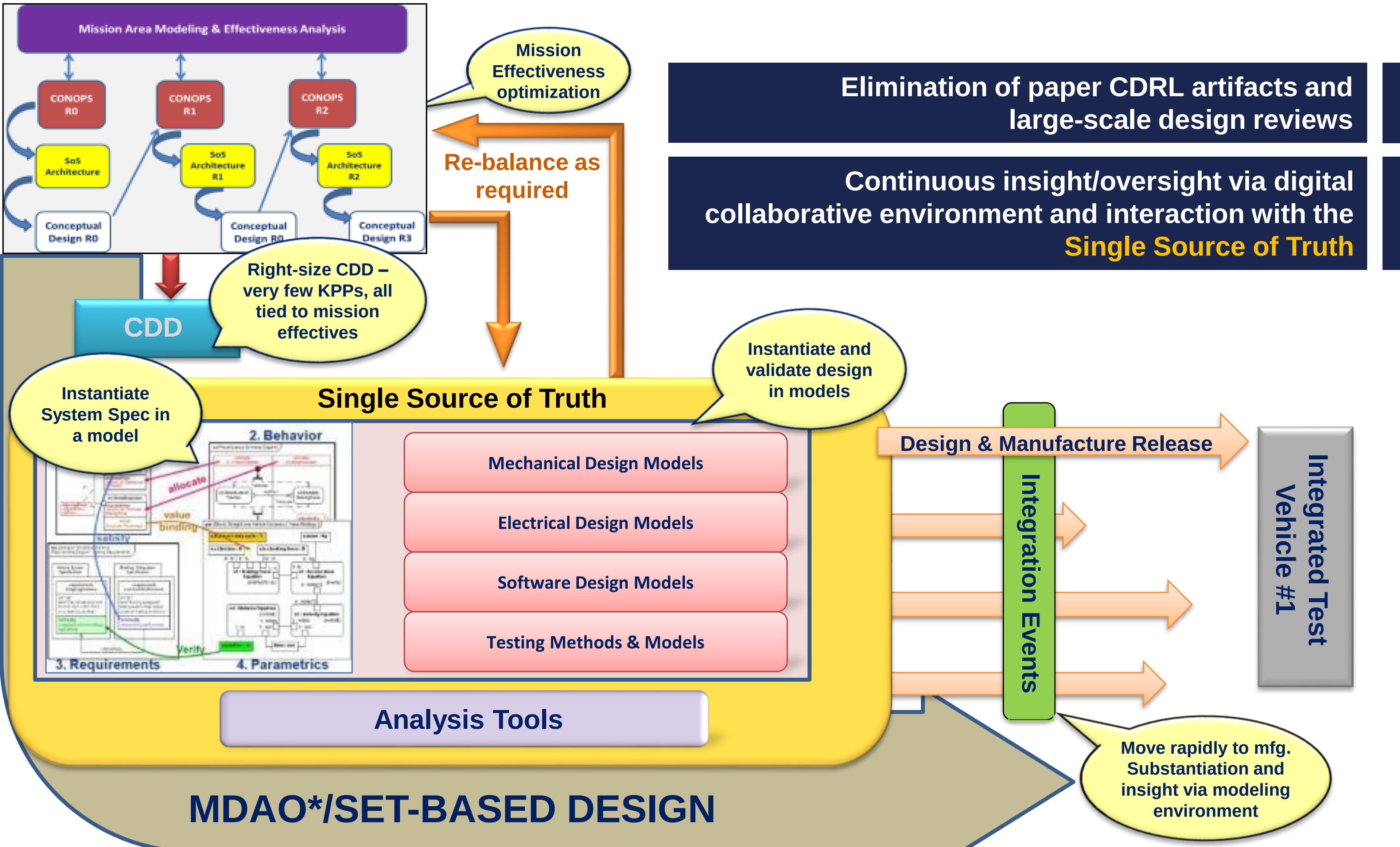
FLIGHT TEST

INTEGRATION LABORATORY

INSTALLED SYSTEMS TEST FACILITY

LVC-based training required for Fleet integrated ops

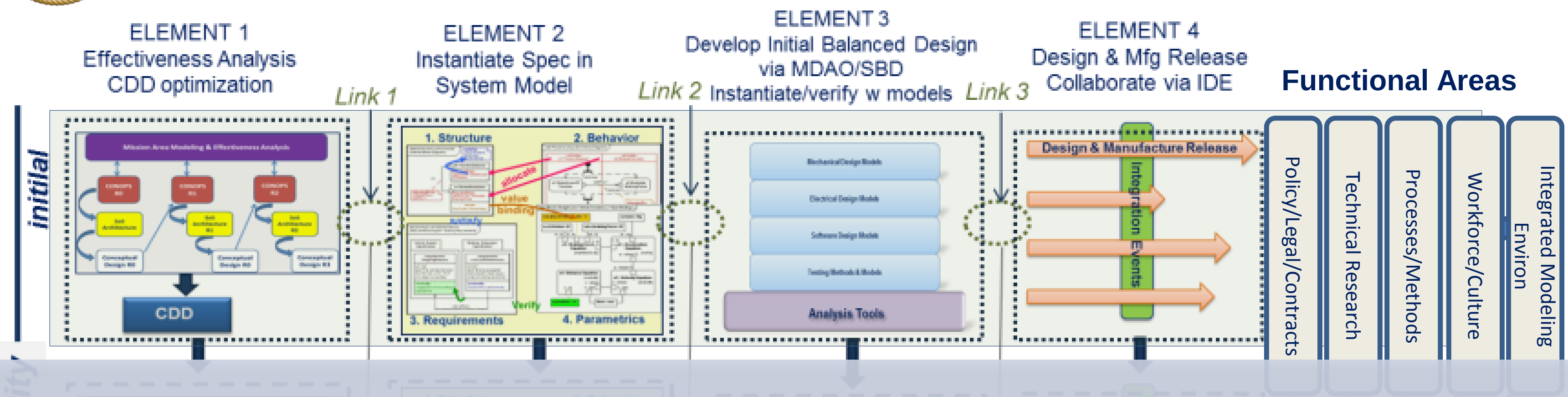
SET Framework



* *Multi-Disciplinary Analysis & Optimization*

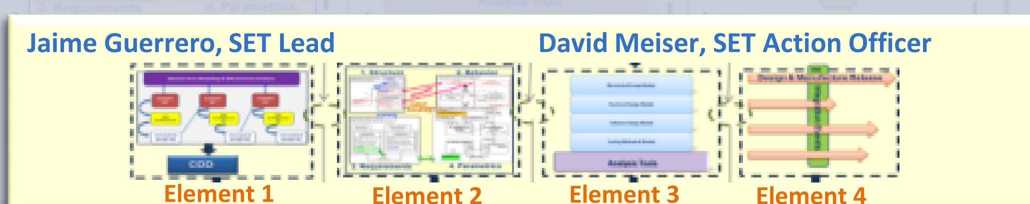
V5.0

Execution Framework



SET Task Framework

Enablers

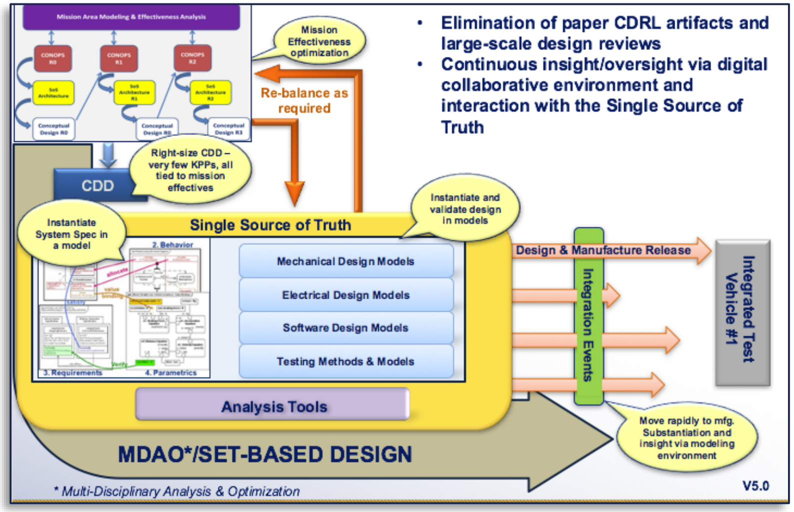


- **SET Research Team** *(Blackburn)*
- **Modeling Env'nt Team** *(Fields)*
- **Workforce/Culture Team** *(Carlson)*
- **Process & Methodology Team** *(Chamberlain/Polakovics)*
- **Policy, Contract, Legal Team** *(Vacant)*
- **SET Framework Links** *(S. Raley)*

Each Element requires work in the 5 Functional Areas in order to reach "Full Maturity"

Surrogate System Experiment

- Simulate Execution of SET Framework
- Use UAV scenario developed in SERC models
  - Combine SysML models already in development – requirements, with functional and logical views
  - Use MDAO of parametrics for some KPPs
    - Consider NATO example
    - Characterize objectives and thresholds
  - Create a model-based contract simulating RFP / SOW
- Use commercial organization to simulate industry organization
  - Refinement of SysML models to reflect corrections / innovations with physical allocation views
  - Integrate with multi-physics-based Initial Balanced Design
  - Simulate continuous virtual reviews and derive new objective measures for assessing maturing design
- Simulate source selection based on dynamic models and simulations



Industry-Government Partnership

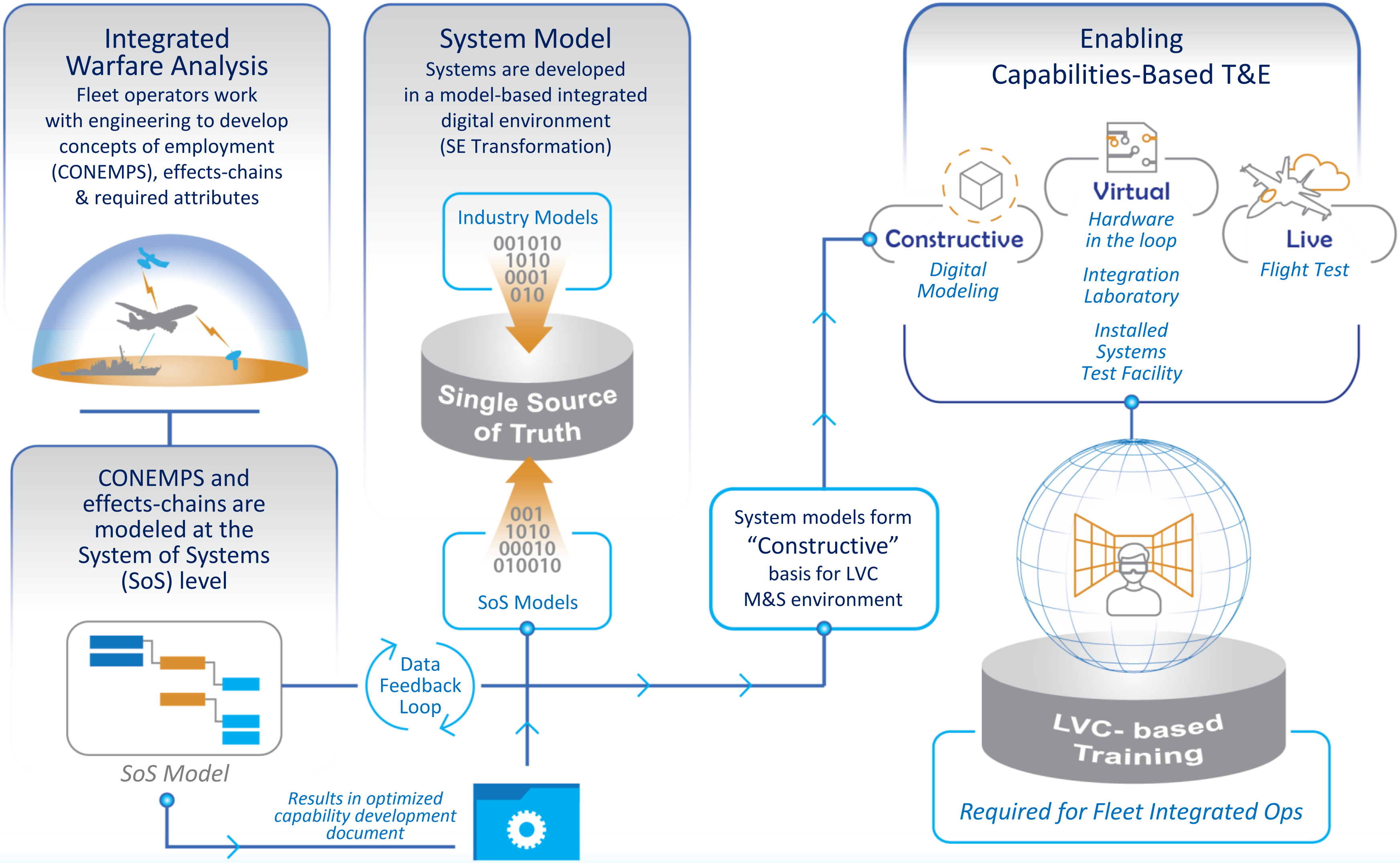
- SET applies to both Government and Industry

- Government must reassess its role in the acquisition process and the methods for executing that role
  1. Criteria for gov't involvement / oversight (not every decision)
  2. If involved, must be on developer's timeline
  3. Must bring value to the decision – not just positional authority

- Industry must fully leverage advances in HPC-enabled models and participate in establishing a collaborative, integrated digital environment which enables continuous interaction

For More Information, Contact:
Mr. Dave Cohen, Director Systems Engineering
(301) 757-5542
david.cohen@navy.mil

Capabilities Based Acquisition



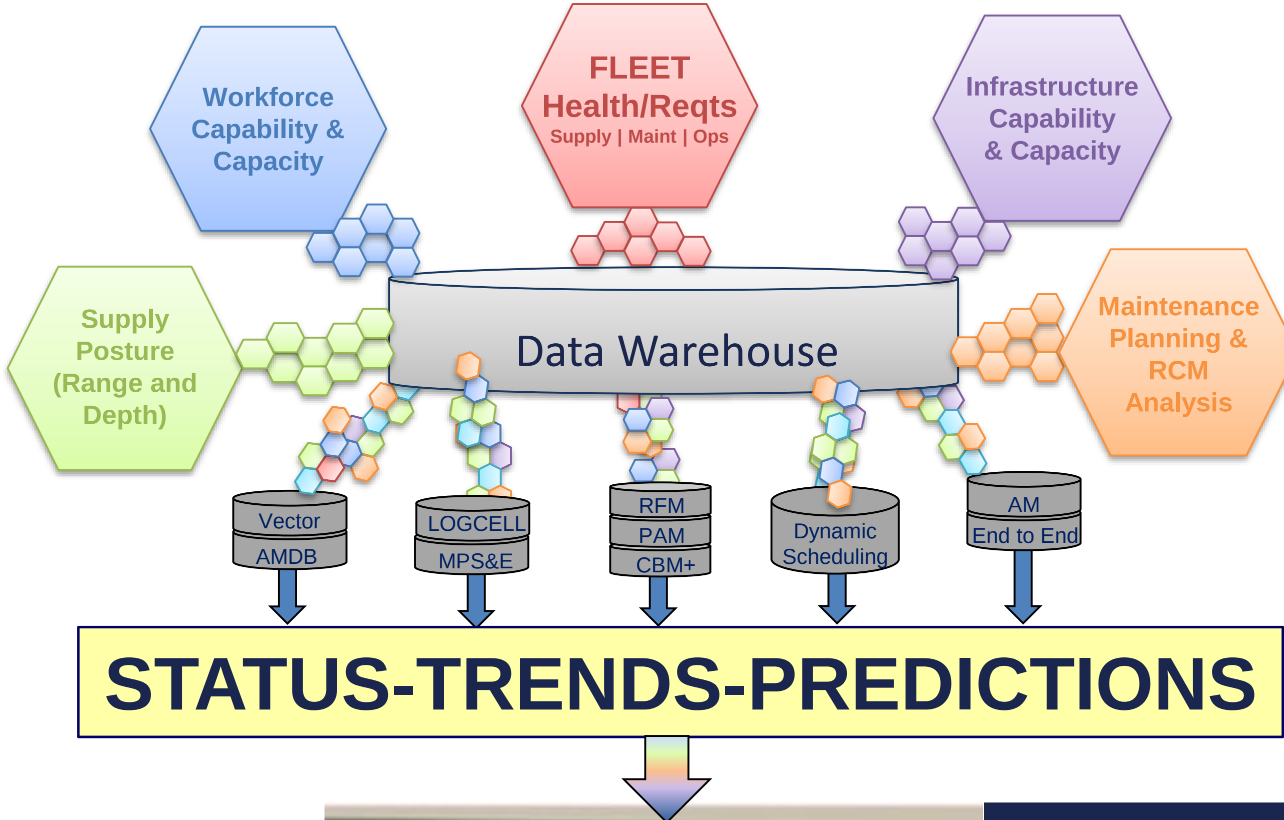
Integrated Digital Environment accelerates delivery of operationally relevant capabilities

Sustainment Vision 2020 – What it Looks Like

RAW DATA

APPLICATIONS / TOOLS

ANALYSIS



FLEET DECISIONS
FLEET SUPPORT

Optimization and Prioritization of Resources to Meet Fleet Needs…
Maintenance Planning
Supply Support
Workforce
Facilities

Universal Information
Faster Decision Making
Predictive Sustainment Planning
Reduced Cost
Increased Readiness

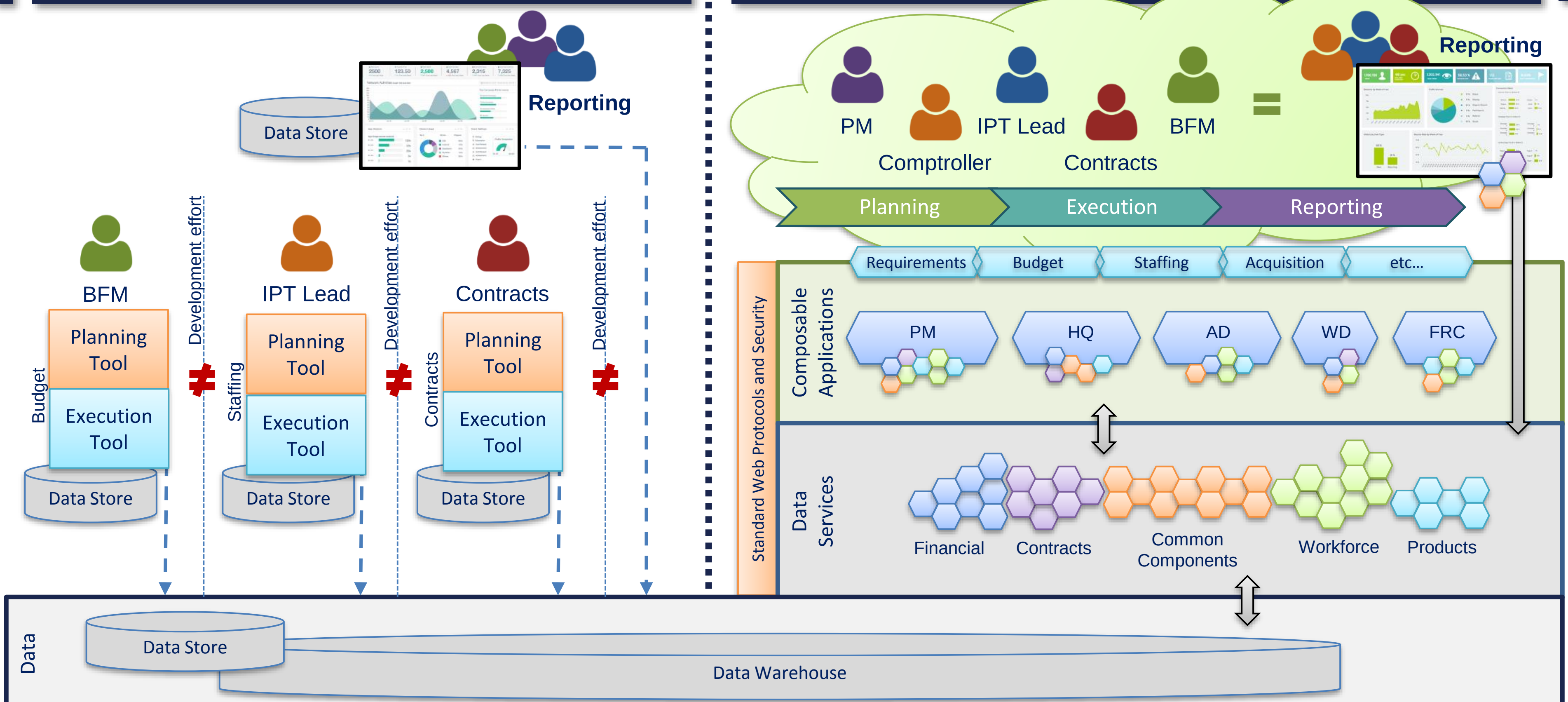
Digital Transformation: Business Operations

Today: Monoliths in Silos

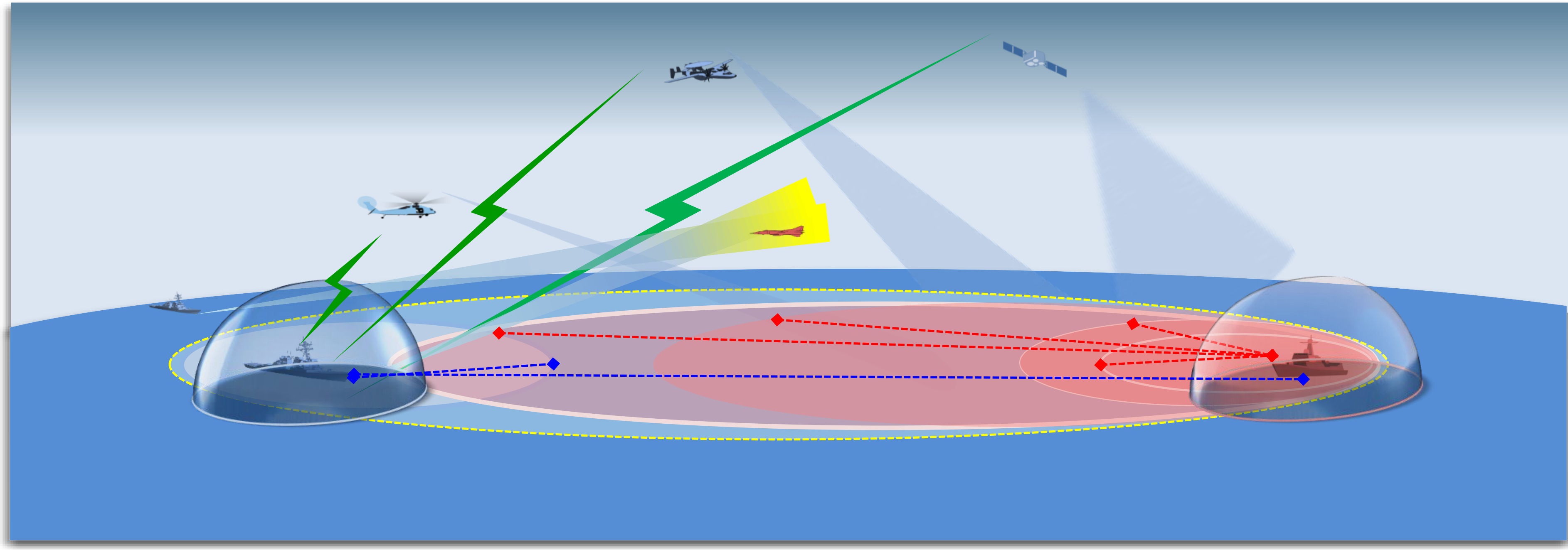
- Applications built in silos
- Data duplicated in tools causing manual re-entry
- Data locked in tools preventing ease of re-use
- Application changes slow and costly
- Functionality duplicated across tools causing inconsistencies and difficulty in coordinating business process changes
- Can't tailor to support unique process across business units
- Similar functionality reinvented over and over again at great cost

Tomorrow: The Composable Business

- Infrastructure enables tailored applications while maintaining consistent core business rules and data
- Applications "composed" from reusable services
- Consistency of Data and Business Rules across Business Operations
- Agility in supporting rapid Business Process changes
- Lightweight services with short development lifecycle
- Individual Services "owned" by Authoritative Competency



USN vs PLA(N) Capability Fielding



We're Being Out-Sticked

USN Warfighting Advantage Against PLA(N) has Steadily Eroded

DHS SCIENCE AND TECHNOLOGY

DHS Systems Engineering Acquisition Challenges and Issues

Homeland Security

Science and Technology

NDIA 20th Annual National SE Conference

October 25, 2017

James D. Tuttle

Chief Systems Engineer

Science and Technology Directorate

Department Homeland Security

Major DHS Operating Components

- Transportation Security Administration (TSA)
- U.S. Coast Guard (USGC)
- U.S. Secret Service (USSS)
- U.S. Customs and Border Protection (CBP)
- U.S. Citizenship and Immigration Services (CIS)
- U.S. Immigration and Customs Enforcement (ICE)
- Federal Emergency Management Agency (FEMA)
- Domestic Nuclear Detection Office (DNDO)

TSA Programs

Electronic Baggage Screening Program

Passenger Screening Program

USCG Air Programs

C27-J

HC-144

HC-130J

MH-60J

HH-65

USCG Surface Programs

Fast Response Cutter

Motor Lifeboat

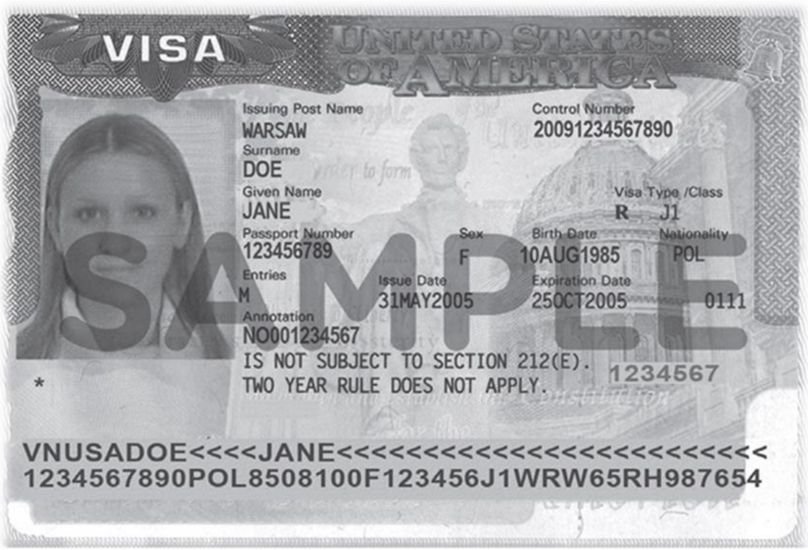
National Security Cutter

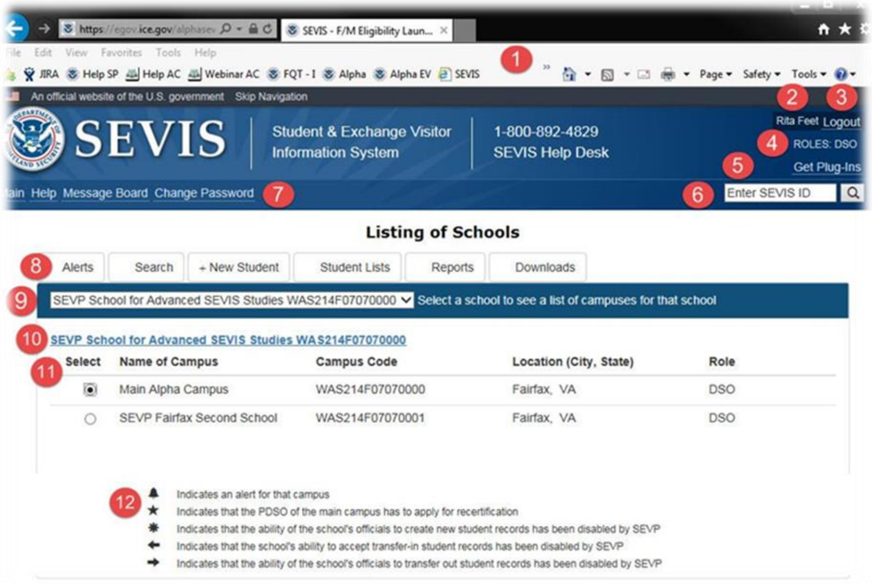
Offshore Patrol Cutter

Heavy Polar Icebreaker

ICE Programs

Student and Exchange Visitor Information System





FEMA Programs

Integrated Public Alert and Warning System

National Flood Insurance Program

Grants Management Modernization

Logistics Supply Chain Management System

USCIS Programs

Transformation Program

CBP Programs

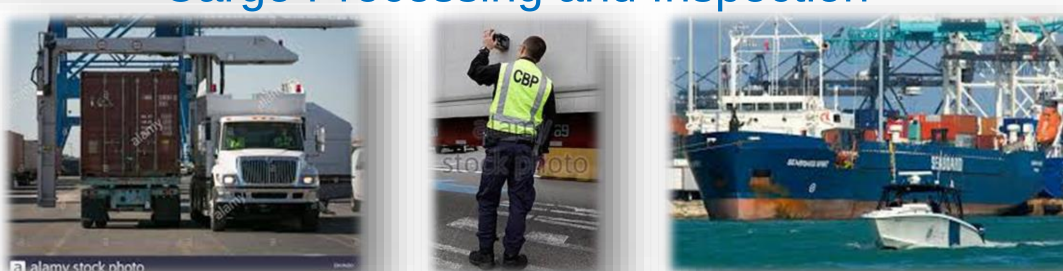
Biometric Entry-Exit

Cross-Border Tunnel Detection

Border Wall

Video Surveillance Systems

Cargo Processing and Inspection



SE Challenges in DHS

- Solutions encompass the entire Homeland Security Enterprise (HSE)
  - Diverse customer base, with different rules, restrictions, and users
  - Diverse “mission set” including security, immigration, trade/commerce, disaster planning, and response
- Significant IT and Embedded/Mixed IT Solutions
  - Privacy and security concerns related to sharing data
  - Controlling proprietary, business, or law enforcement-sensitive data
- Flexible and resilient solutions to respond to emergent threats and national disasters
- Procurement vs. acquisition mentality in many parts of the HSE
- Too much focus on compliance/templates vice critical analysis

SE Staffing Challenges

- DHS has a Level I, II, III SE Acquisition Certification program and activity instructing courses
  - Inconsistency/limited participation
- No consistent SE staffing within Acquisition programs and Component Acquisition oversight offices
- Secretary directed all major acquisition programs and Component Acquisition oversight offices to resource SE expertise
  - Initiative established in Secretary's FY19-23 Resource Planning Guidance (for Components developing Resource Allocation Plans)

SE Challenges in DHS Acquisition Programs

Weak Solution Analysis/Analysis of Alternatives prior to approval

AoAs have not been properly scoped and executed

- Frequently focused on all COTS, no COTS, or a mix, vice analyzing the operational and technical solution space
- Poor definition of alternatives and evaluation criteria
- Relative ranking of alternatives among each other vice against actual mission need/requirements

- AoAs often not informed by data from pilots/prototypes/testing

- AoAs as a process to document the acquisition, vice analyze, learn, and modify to enable better decisions

SE Challenges in DHS Acquisition Programs

Poorly developed Operational Requirements and CONOPS

- Limited CONOPS scope
  - Scenarios do not describe the complete operation or even all the tasks the proposed solution must perform (only small mission tasks that need improvement)
  - Boundaries, interfaces, key external stakeholders/systems of the proposed solution not clearly defined/understood
- Limited analysis leading to the actual Operational Requirement
  - Often not operationally focused
  - Often focused on “user needs” that reflect specific problems
  - Limited analysis to support Threshold and Objective performance values

SE Oversight Challenges

- HQ oversight has heavily focused on programmatic oversight
  - Focused on checklists and artifact existence
  - Limited evaluation of the quality/substance of artifacts
- In 2015, Secretary directed S&T to conduct Technical Assessments on major acquisition programs
  - SE-based Technical Assessments of major acquisition programs
  - Focused on quality, not quantity
  - Not *if* a program has operational requirements; are requirements
    - Feasible
    - Clear
    - Testable
    - Backed by objective analysis
  - Complements existing acquisition programmatic oversight processes
  - Conducted prior to commencement of design/development/integration

Technical Assessment Impacts

- Greater up-front analysis = technically stronger programs
  - Threshold and objective parameters of operational requirements, backed by objective analysis
  - CONOPS that better describe end-to-end system operation, not only parts of the system
  - Trade-off analysis during the Analysis of Alternatives that informs/refines operational requirements and CONOPS
- Holistic (programmatic and technical) perspective for Acquisition executives before design/development/integration activities
- More informed decision-making by Acquisition executives

Conclusion

- DHS enterprise has a wide range of mission areas and a civilian/law enforcement culture
- Acquisition still somewhat synonymous with procurement
- DHS realizes SE needs to be institutionalized across the Department and is making headway
- Developed rigorous SELC Guidance
- Implemented Technical Assessments for Major Acquisition Programs
- AoA, ORDs, CONOPS, etc. improving as SEs engage
- Looking to continue collaboration across government and industry

Homeland Security

Science and Technology

Headquarters U.S. Air Force

Integrity - Service - Excellence

NDIA Systems Engineering Conference

Line of Action (LOA) 2 Action Plan

25 Oct 17

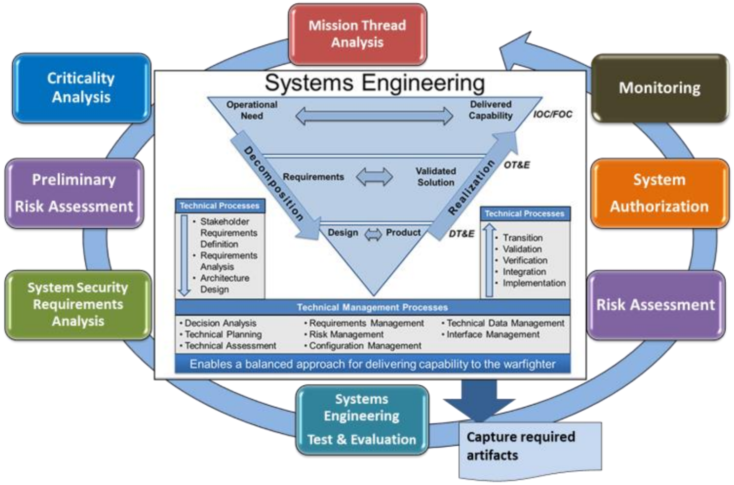
Dr. Ken Barker, SL
AFLCMC/EZ
DSN: 785-7213

LOA 2
Goal & Objectives

- **Goal: Efficiently and effectively incorporate Systems Security Engineering (SSE) into the Systems Engineering (SE) process in all phases of the Acquisition Lifecycle to increase cyber resilience in AF systems**
- **Team Members: AFLCMC, AFTC, SMC, NWC, AFMC, AFRL, SMEs**
- **Objectives**
  1. **Process Integration:** Integrate SSE into SE processes and deliverables
  2. **Process Assessment:** Develop metrics to measure SSE incorporation into SE processes and deliverables
  3. **Product V & V:** Develop system cyber test and evaluation methodology and capability across the lifecycle for all AF systems - aircraft, weapons, C4ISR, IT, Space, Nuclear

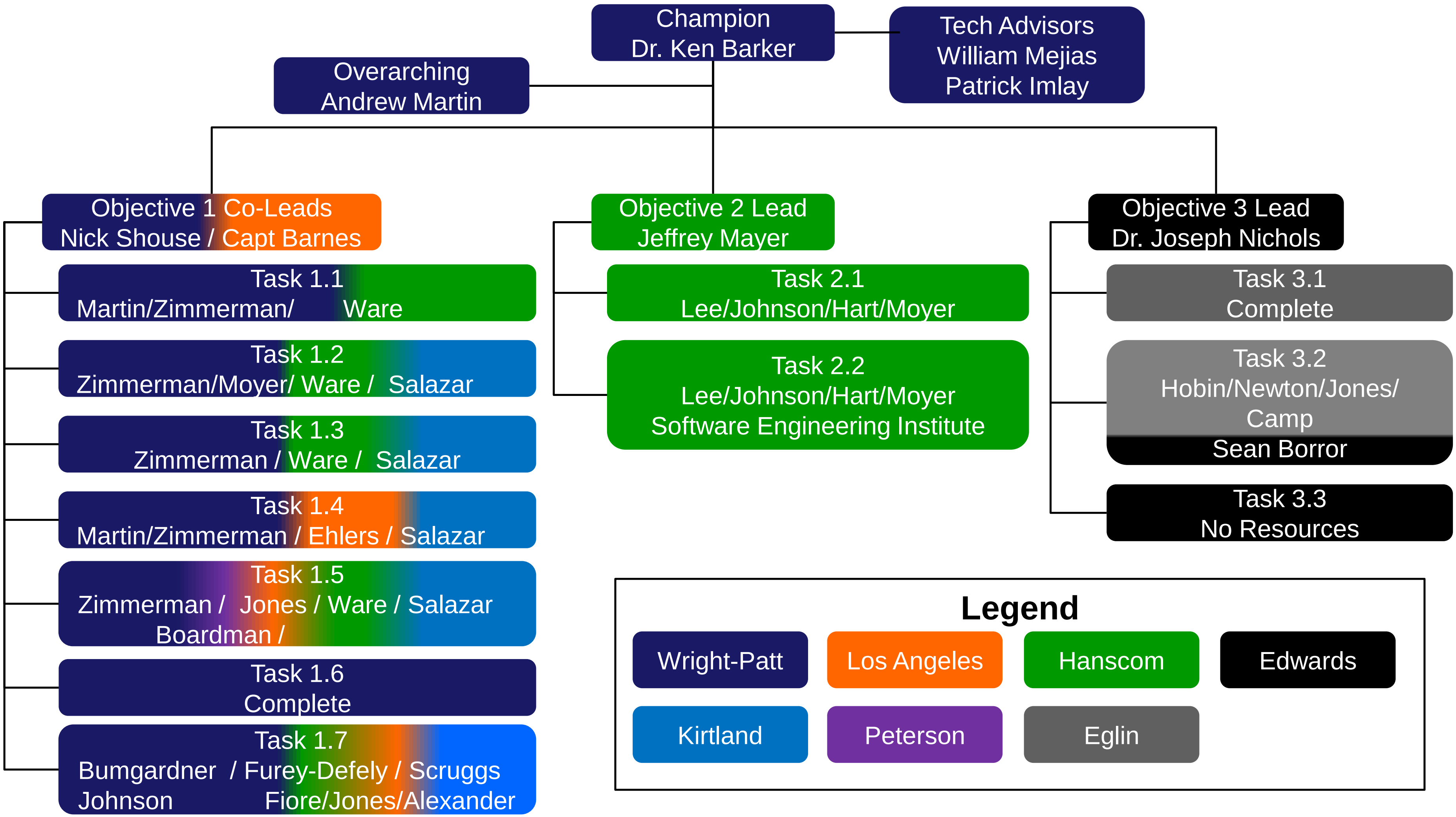
LOA 2
Integrate SSE into SE Processes

- **Status:**
  - Identified OPRs & formalized membership
  - Implementing Action Plan
  - Several process guides drafted/in coordination
  - SE Tech Review entry/exit criteria drafted
  - Cyber scorecard drafted; pilot apps under way
  - Cyber Test & Evaluation Study Completed



- **Near-term Way Ahead:**
  - Update existing guides based on feedback and evolving policy/regulations
  - Produce deliverables and work with Cyber Resiliency - Technical Advisory Council (CR-TAC) to disseminate/ institutionalize
  - Continue interfacing across LOAs, especially with the LOA 3 Cyber Resiliency Support Team (CRST)

LOA 2 Organization



Objective 1: Process Integration

- **Objective Description:** Integrate SSE principles into SE processes and deliverables
- **OPRs:**
  - Leads: Mr. Nick Shouse, AFLCMC/EZS;
    Capt Cameron Barnes, SMC/ENX
  - Reps from AFLCMC, SMC, AFNWC, AFMC, FFRDCs, Contractor SMEs

LOA 2 Input-Output

Input

- FAA
- NIST
- AO/CSAs
- LOA 6
- NDAA 1647
- CICC/CPT
- LOA 3

Processing

- LOA 2
- Task 1.2
- Task 1.7
- Task 3.2

Output

- System Requirements Document
- System Performance Specification
- Statement of Work tasks
- Required deliverables
- Etc.

LOA 2, Task 1.1

Establish executable process for CPI & CC ID

Task Description & Deliverables

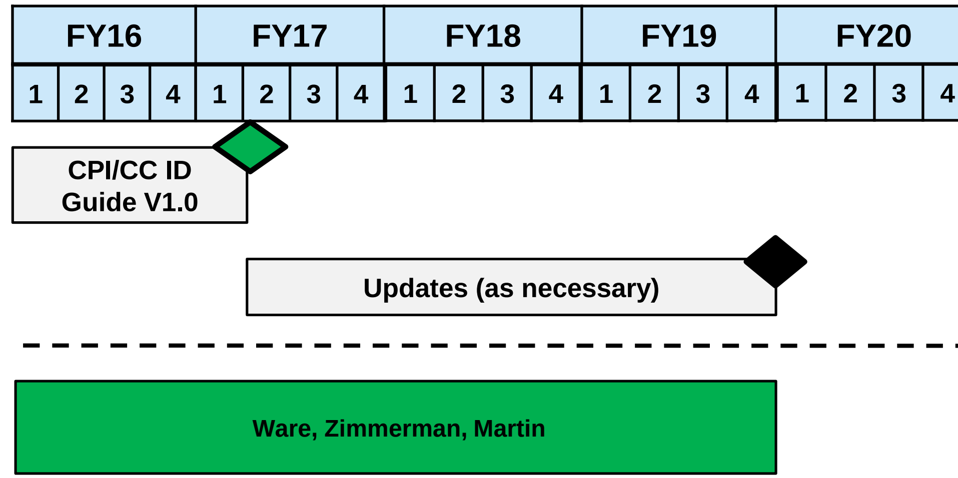
Description

- Provide process guidance that enables programs to accurately identify and obtain independent review and validation of CPI/CC.

Deliverables

- CPI and CC Identification Process Guide

Resource Loaded Schedule



Done Criteria

- Approval of CPI/CC Identification Process Guide by CR-TAC
- CPI/CC Identification Process Guide submitted for consideration to SAF/AQR for adoption as an Air Force Pamphlet (AFPAM) or referenced by AFPAM 63-113, Program Protection Planning for Life Cycle Management
- Guide posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, and SSEs
- Training – Analyze whether existing module of Program Protection course on CPI/CC ID is sufficient
- Accountability – Best practice to ensure correct implementation of DoDI 5200.39 and 5200.44
- Sustainment organization – Transition in FY19 or 20 to AFLCMC/EZSP and SMC/ENX for sustainment

LOA 2, Task 1.2

Define SSE & Integrate SSE into SE

Task Description & Deliverables

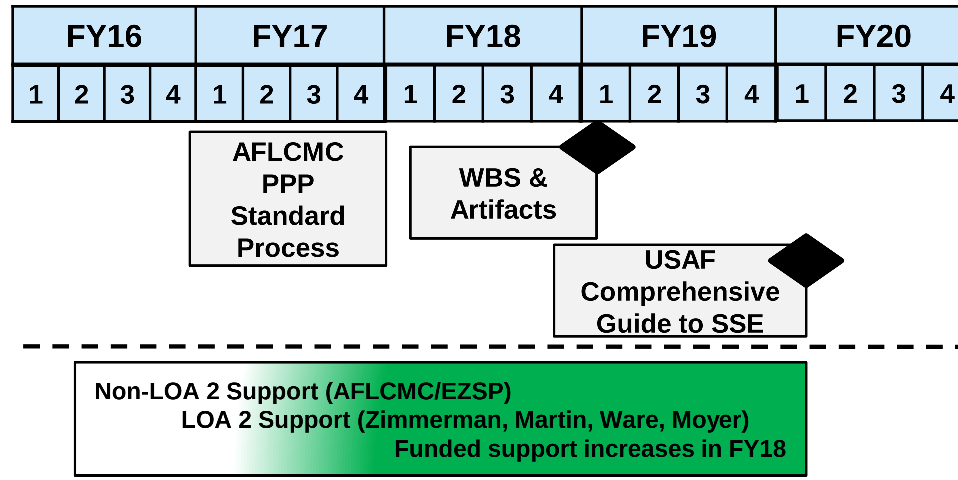
Description

- To provide understanding of SSE terms and concepts within a *Guide for Accomplishing Comprehensive SSE*

Deliverables

- Guide for Accomplishing Comprehensive SSE, including Program Work Breakdown Structure (WBS), artifacts, and templates

Resource Loaded Schedule



Done Criteria

- Approval of the Guide for Accomplishing Comprehensive SSE by CR-TAC
- Submitted to SAF/AQR for consideration as a replacement for the existing AFPAM 63-113 (*Program Protection Planning for Life Cycle Management*)
- Guide posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, and SSEs
- Training – Potentially add module to Program Protection course
- Accountability – Recommended to PEOs as a best practice
- Sustainment organization – Transition in FY20 to AFLCMC/EZSP and SMC/ENX for sustainment

LOA 2, Task 1.3

Establish executable process for System Security Risk Management

Task Description & Deliverables

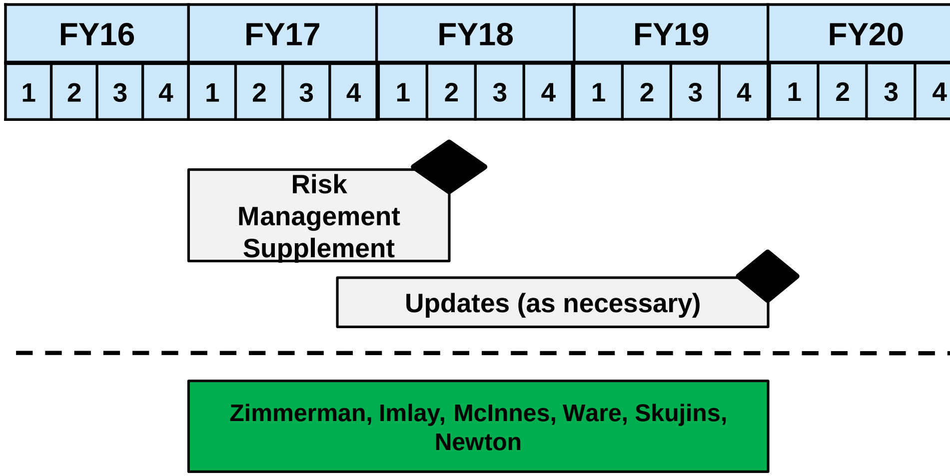
Description

- Provide one integrated system security risk management process that programs execute as part of their overarching risk management process, including the steps for risk planning, identifying, analyzing, handling, and monitoring.

Deliverables

- Risk Management Supplement to AFPAM 63-128, Integrated Life Cycle Management - Supplemental guide to integrate system security risk management

Resource Loaded Schedule



Done Criteria

- Approval of the Risk Management Supplement by the CR-TAC
- Submitted for consideration to SAF/AQR for update of the AFPAM 63-128, Integrated Life Cycle Management, to include system security risk management
- Supplement posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs
- Training – TBD
- Accountability – Recommended to PEOs as a best practice
- Sustainment organization – Transition in FY19 or 20 to AFLCMC/EZAS and SMC/ENX for sustainment

LOA 2, Task 1.4

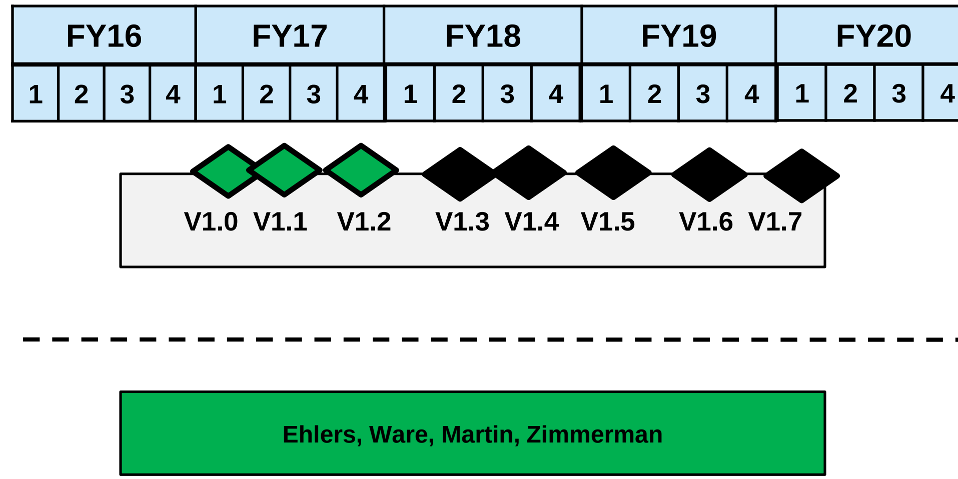
Develop and execute acquisition language guidance

Task Description & Deliverables

Description
- Provide SSE-focused guidance to program offices for use in various acquisition docs
  - Offers programs a common starting point

Deliverables
- USAF SSE Acquisition Guidebook – Iterative development with periodic publication of updated versions

Resource Loaded Schedule



Done Criteria

- Interim deliveries/updates made as new information becomes available from other Cyber Campaign Plan activities
- Approval of the Final USAF SSE Acquisition Guidebook by CR-TAC
- Guide posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, SSEs, and Contracts
- Training – TBD
- Accountability – Recommended to PEOs as a best practice
- Sustainment organization – Transition in FY20 to AFLCMC/EZSI and SMC/ENX for sustainment

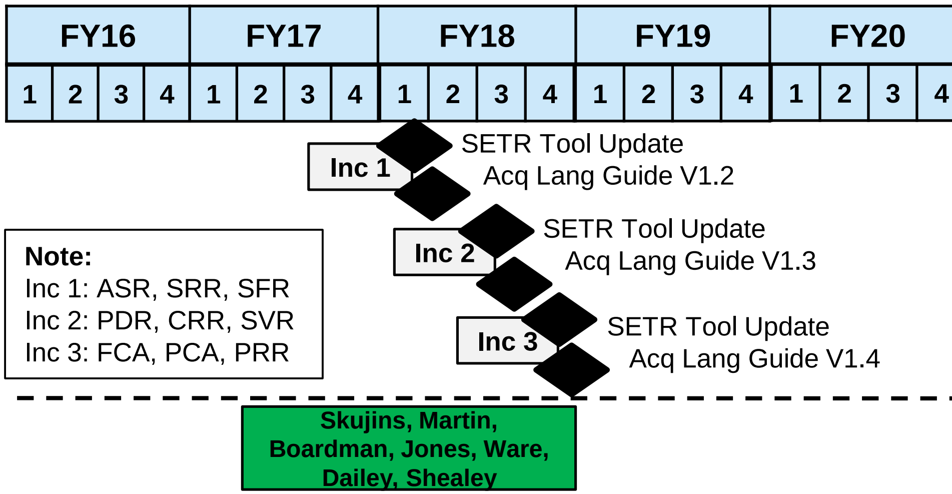
LOA 2, Task 1.5
Establish SETR SSE Entry & Exit Criteria

Task Description & Deliverables

Description
- Establish SETR SSE entry/exit criteria that program offices across AFLCMC, SMC, and AFNWC can use to evaluate the design maturity of programs during various SETR activities.

Deliverables
- Updated SETR SSE Entry/Exit Criteria/Tasks outlined within the USAF SSE Acq Guidebook
- Updated SETR Toolset with SSE Entry/Exit Criteria

Resource Loaded Schedule



Done Criteria

- Final SETR Entry/Exit Criteria reviewed/approved by the CR-TAC
- Update of AFLCMC SETR Toolset with approval by AFLCMC/EZSI

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, and SSEs
- Training – TBD
- Accountability – Recommended to PEOs as a best practice
- Sustainment organization – Transition of SSE Acq Guidebook in FY20 to AFLCMC/EZSI and SMC/ENX for sustainment. SETR Toolset will be continue to be maintained by AFLCMC/EZSI.

LOA 2, Task 1.6 (COMPLETE)

Provide recommended system security language for ICDs, CDDs, and CPDs

Task Description & Deliverables

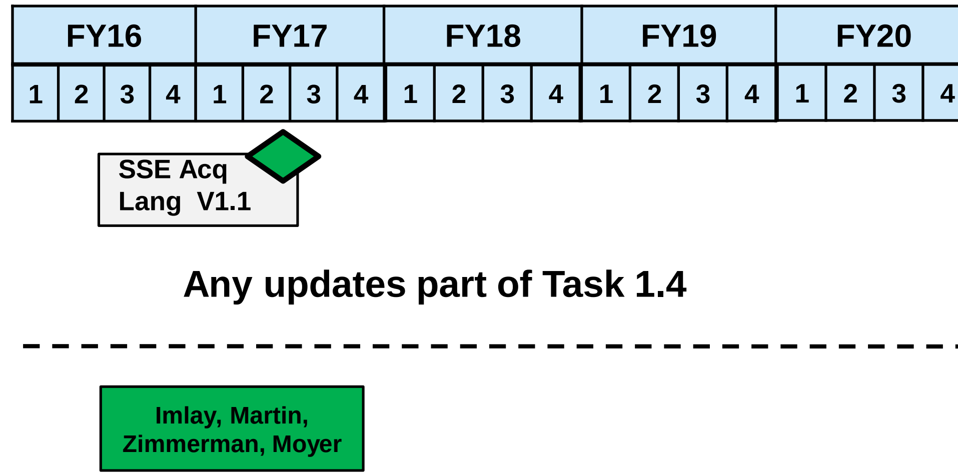
Description

- Create guidance that enables program offices to interact with users and inform the development of weapon system requirements that account for SSE activities throughout the acquisition life cycle.

Deliverables

- Updated SSE Acquisition Guidebook identifying process owners; summaries of applicable requirements development processes; and sample ICD, CDD, and CPD requirements language

Resource Loaded Schedule



Done Criteria

- Approval of USAF SSE Acquisition Guidebook v1.1 by the CR-TAC

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, and SSEs
- Training – See Task 1.4
- Accountability – See Task 1.4
- Sustainment organization – See Task 1.4

LOA 2, Task 1.7

Develop system and acquisition security requirements for programs

Task Description & Deliverables

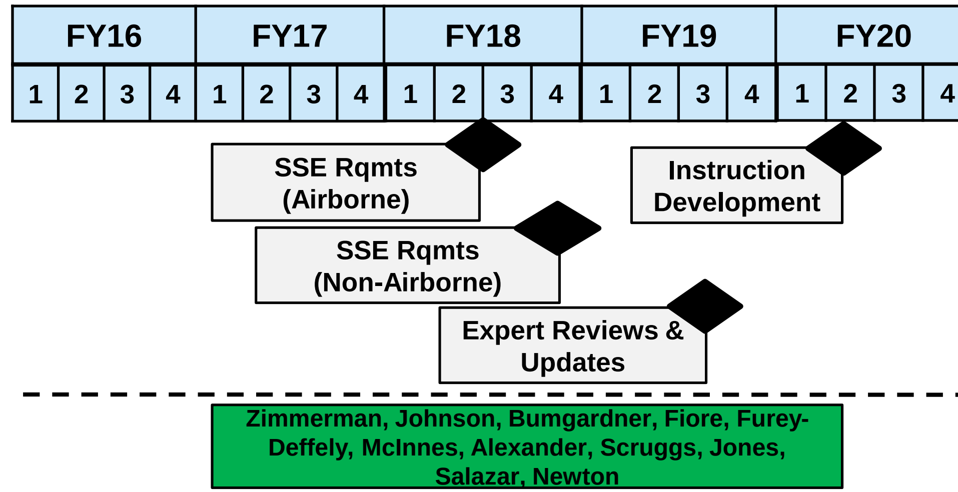
Description

- Develop a requirements construct modeled after the format used in (MIL-HDBK) 516C, that focuses on criterion, standards, methods of compliance (i.e., verification), and references.

Deliverables

- Traceable to NIST controls for reciprocity and audit purposes.
- Aligned with various domain frameworks
- An USAF-wide solution that includes areas of domain-agnostic requirements

Resource Loaded Schedule



Done Criteria

- Approval of the Final SSE Requirements Construct by CR-TAC
- Construct posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, and SSEs
- Training – Guidance/instruction on use of Construct
- Accountability – Potentially update Air Force Instruction 17-101 or other instruction
- Sustainment organization – Transition in FY20 to AFLCMC/EZSI and SMC/ENX for sustainment

Objective 2: Process Assessment

- **Objective Description:** Develop metrics to measure SSE incorporation into SE processes and deliverables
- **OPR:**
  - Lead: Mr. Jeff Mayer, AFLCMC/EZC
  - Representatives from AFLCMC, SMC, NWC, DOEs

LOA 2, Task 2.1

Develop a Cyber Health Scorecard to measure SSE process health within program offices

Task Description & Deliverables

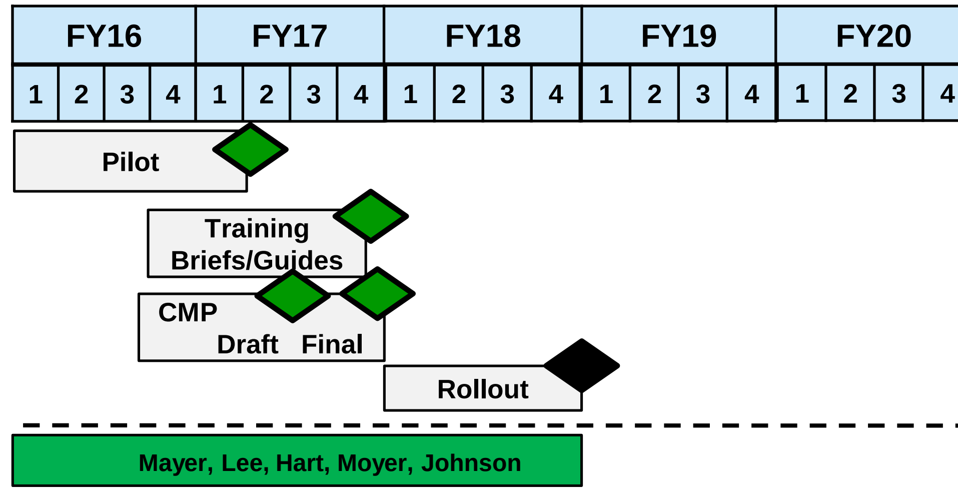
Description

- Develop scorecard for program office use
  - Enable programs to evaluate quality of applied programmatic practices

Deliverables

- Final Enhanced Guidance
- Updated Overview and Training briefings
- Health Scorecard Configuration Management Plan
- Cyber Health Scorecard

Resource Loaded Schedule



Done Criteria

- Final Cyber/SSE Health Assessment reviewed/approved by the CR-TAC
- Guidance recommending use of tool sent by CROWS or SAF/AQR to PEOs
- PEO Enterprise Roll-up Capability integrated into tool
- Assessment posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, including PMs, System Program Directors, & PEOs
- Training – Narrated training briefs and enhanced guidance
- Accountability – Memorandum from SAF/AQR to PEOs encouraging use of assessment
- Sustainment organization – Potential transition in FY19 to AF SE Assessment Model (SEAM) and managed by AFMC/ENS and SMC/ENE

LOA 2, Task 2.2

Develop methodologies & metrics to measure our systems' security and resiliency

Task Description & Deliverables

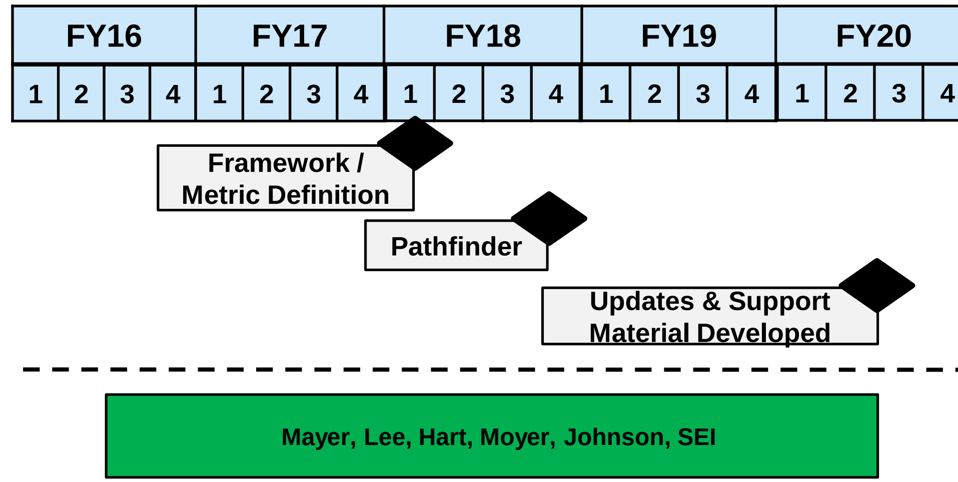
Description

- Form an AF-level Cybersecurity Metrics Framework
    - Allows capturing and summing metrics to provide system and/or platform level insight
    - Conduct pathfinders, refine metrics, and instantiate a collection tool & analysis method

Deliverables

- AF Cyber Metrics Framework

Resource Loaded Schedule



Done Criteria

- Final AF Cyber Metrics Framework reviewed/ approved by the CR-TAC
- Framework posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, including PMs, System Program Directors, & PEOs
- Training – TBD
- Accountability – TBD
- Sustainment organization – TBD

Objective 3: Product V&V

- **Objective Description:** Develop system cyber test and evaluation methodology and capability across the lifecycle for all AF systems - aircraft, weapons, C4ISR, IT, space, nuclear
- **OPR:**
  - Dr. Joe Nichols, AFTC/CZ
  - Reps from AF/TE, AFOTEC, AFMC, AFLCMC, SMC, NWC, AFRL, NASIC, DOEs

LOA 2, Task 3.1 (COMPLETE)

Monitor & provide Cyber T&E Study

Task Description & Deliverables

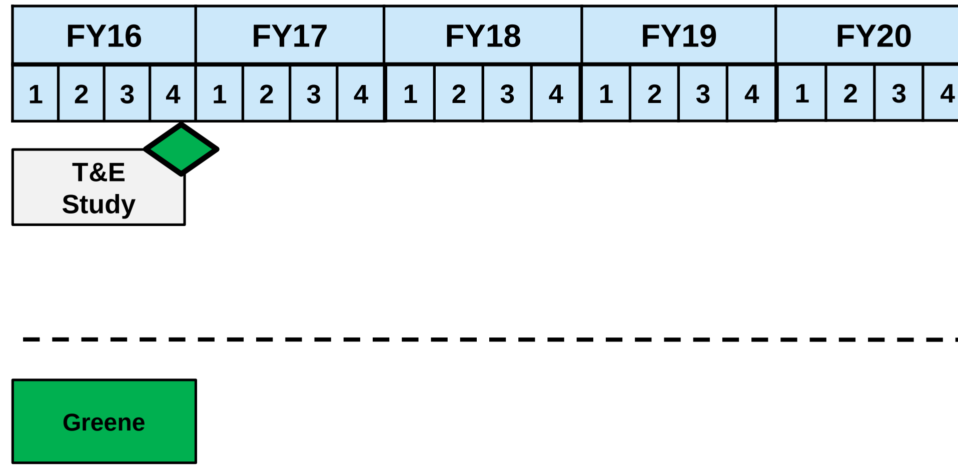
Description

- Complete Cybersecurity Test and Evaluation (CTE) Study under guidance of 46th Test Squadron
  - Identify environment, infrastructure, tools, methodology, manpower, & resources required

Deliverables

- Cyber T&E Study
  - Capability and infrastructure gaps
  - Process recommendations & investment map
  - Manpower study on required expertise and workforce requirement

Resource Loaded Schedule



Done Criteria

- Completion of the Cyber T&E Study to inform investment planning and task 3.2

Institutionalization

- The Cyber T&E Study is complete and maintained by the 46 TS. Analysis will be used to inform investment planning and task 3.2

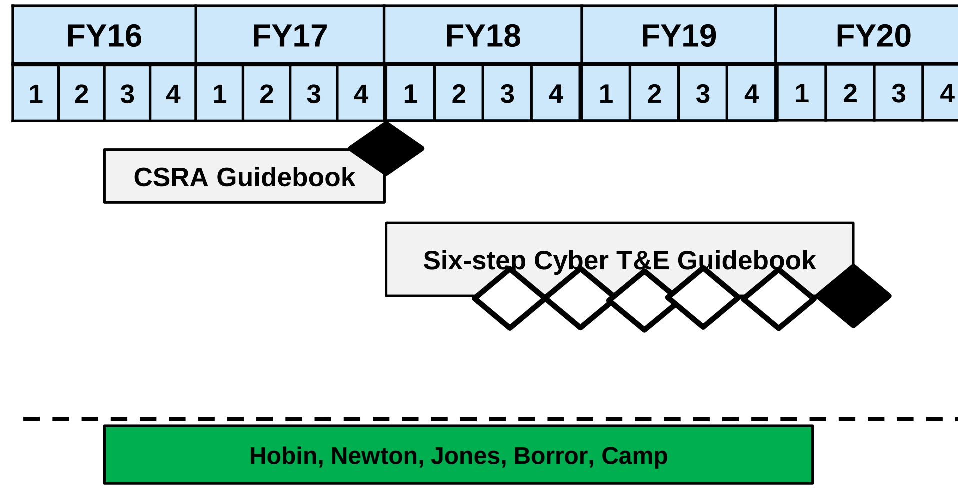
LOA 2, Task 3.2
Cyber Test Technique Development

Task Description & Deliverables

Description
- Develop cybersecurity test strategies, document best practices and lessons learned, and produce a cybersecurity test techniques handbook

Deliverables
- Cyber System Risk Assessment Guidebook
- Cyber T&E Guidebook

Resource Loaded Schedule



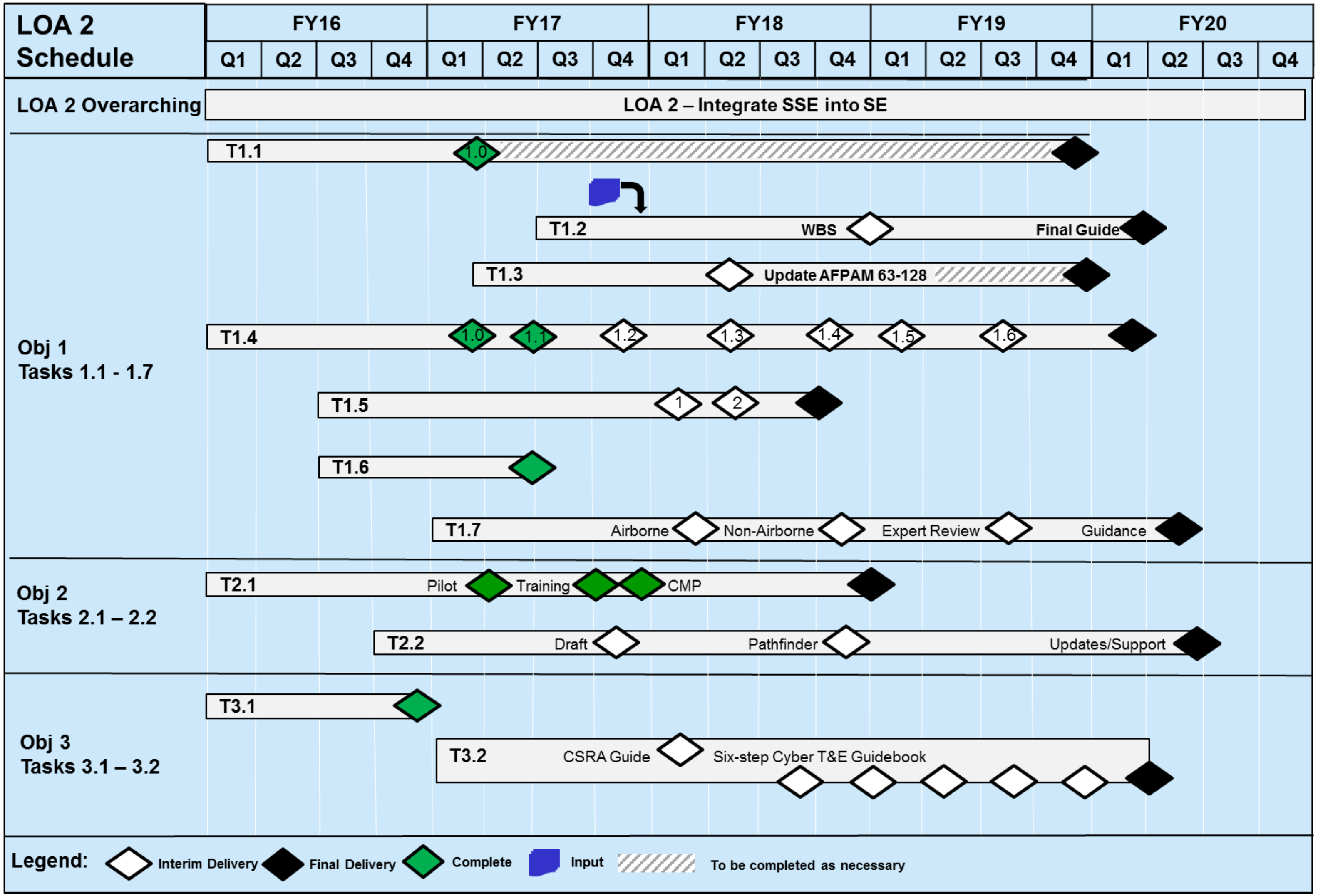
Done Criteria

- All guidebooks and methodology approved for use by Headquarters AF/T&E
  - 46 TS coordination and comment resolution completed
  - Internal LOA 2 coordination and comment resolution completed
  - Cross-LOA coordination and comment resolution completed

Institutionalization

- Targeted Audience – Acquisition center program office and Air Force Test Center, especially 46 TS
- Training – TBD
- Accountability – TBD
- Sustainment organization – Transition upon completion to the 46 TS for sustainment

Schedule



LOA 2 Schedule
FY16 FY17 FY18 FY19 FY20
Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4
LOA 2 Overarching
LOA 2 – Integrate SSE into SE
T1.1
1.0
T1.2
WBS
Final Guide
T1.3
Update AFPAM 63-128
T1.4
1.0 1.1 1.2 1.3 1.4 1.5 1.6
Obj 1
Tasks 1.1 - 1.7
T1.5
1 2
T1.6
T1.7
Airborne
Non-Airborne
Expert Review
Guidance
Obj 2
Tasks 2.1 – 2.2
T2.1
Pilot
Training
CMP
T2.2
Draft
Pathfinder
Updates/Support
Obj 3
Tasks 3.1 – 3.2
T3.1
T3.2
CSRA Guide
Six-step Cyber T&E Guidebook
Legend:
Interim Delivery
Final Delivery
Complete
Input
To be completed as necessary

Digitally Transforming Aerospace & Defense

Tim Walden
Lockheed Martin Fellow
Chief Engineer, Corporate Engineering & Production Operations

“Change is the law of life. And those who look only to the past or present are certain to miss the future.”

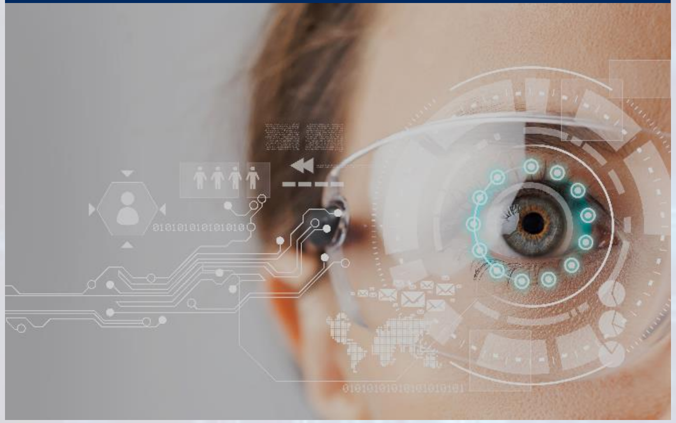
JOHN F. KENNEDY

Reshaping Industrial Operations

Advanced Design Synthesis

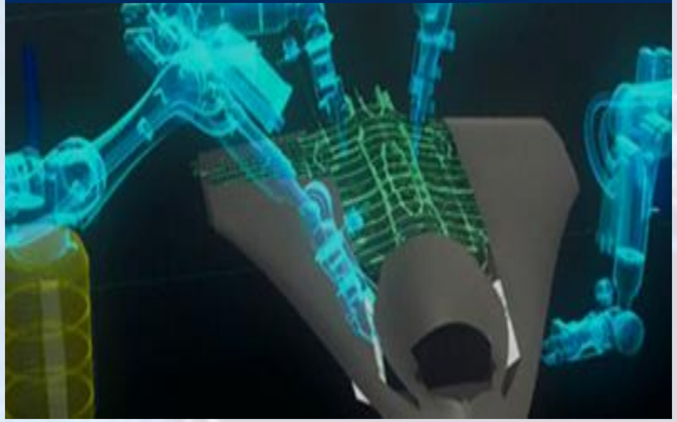
Cognitive Assistants

Human Augmentation



Designer Materials

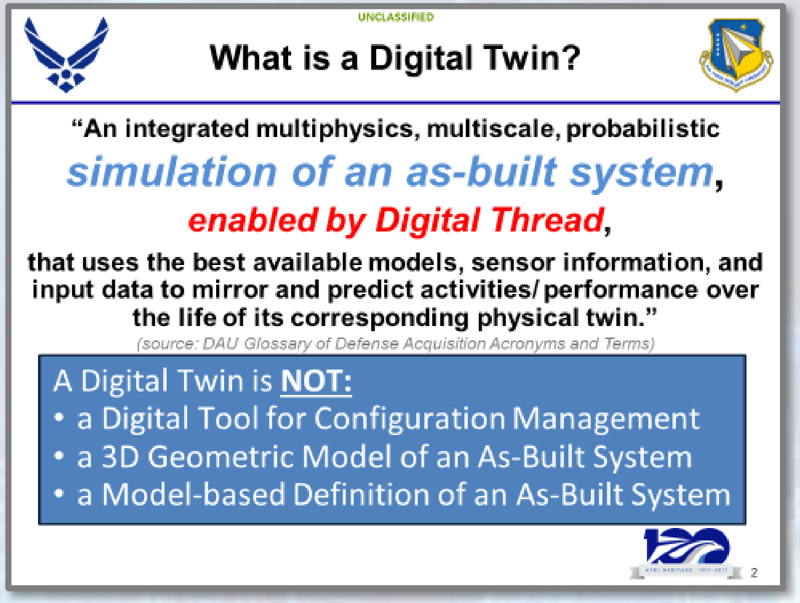
Intelligent Machines

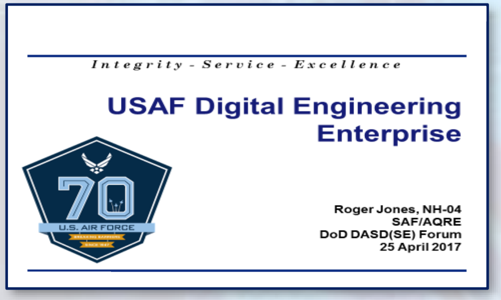


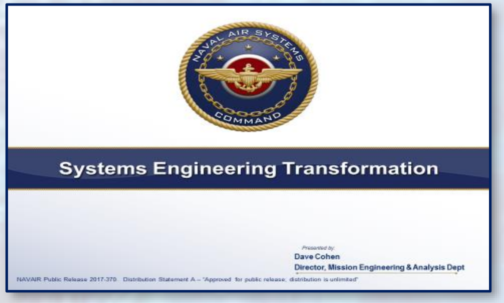
Transformative Computing

Machines evolving from tools to trusted human peers

Government on the Same Journey







A Call to Arms

- **We must transition to a structured, digital relationship, with haste**
  - **The integrated digital models must be the unambiguous source of truth**
  - **Models, and their data and simulations, live forever**
  - **Provide the necessary context for future use**
- **We must prepare for machines as human force-multipliers**
  - **Structure the data**
  - **Develop the trust**
- **OEMs and Government must find a way to experiment together**
  - **Outside of the competition constraints**
- **We must embrace multiple pipelines for skills**
  - **Explore avenues beyond the 4-year degrees for acquiring new skills**
  - **Exploit technology for rapid skill development and training**

Strategy without tactics is the slowest route to victory.
Tactics without strategy is the noise before defeat.”

- Sun Tzu

Modeling and Simulation in the Systems Engineering Process

A Half-Day Tutorial

Prepared and Presented by:

James E. Coolahan, Ph.D.

Johns Hopkins University Engineering for Professionals

Coolahan Associates, LLC

jim.coolahan@jhu.edu

jim@coolahan.com

410-440-2425 (cell)

Tutorial Learning Objectives

Learning Objectives: At the conclusion of this tutorial, students should be able to:

- Define and distinguish key modeling and simulation (M&S) terms
- Name some ways in which M&S can aid in needs and opportunities analysis
- Illustrate the contents of the five major components of a system effectiveness simulation for a system
- Explain typical applications of simulations in several engineering disciplines
- Identify issues that need to be addressed in planning for M&S use during test and evaluation
- Name some types of models and simulations used in the planning / execution of system production
- Explain how system operation simulations can be used to investigate system anomalies during sustainment

Tutorial Outline

- Part 1: Overview of Modeling and Simulation
- Part 2: Use of M&S by Phase of the Systems Engineering Process
  - M&S in System Needs and Opportunities Analysis
  - M&S in Concept Exploration and Evaluation
  - M&S in Design and Development
  - M&S in Integration and Test & Evaluation
  - M&S in Production and Sustainment

Part 1:
Overview of
Modeling and Simulation

Lecture Outline

- Definitions and Distinguishing Characteristics
- Views and Categories of Models and Simulations
- Resolution, Aggregation, and Fidelity
- Overview of the Model/Simulation Development Process
- Important M&S-Related Processes
- M&S as a Professional Discipline
- Summary

Key Modeling and Simulation Definitions

There are a number of definitions of models, simulations, and modeling and simulation (M&S). For the purposes of this tutorial, we will adopt the definitions published by the U.S. Department of Defense (DoD), below.

- Model: A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. [1]
- Simulation: A method for implementing a model over time. [1]
- Modeling and simulation: The discipline that comprises the development and/or use of models and simulations. [2]

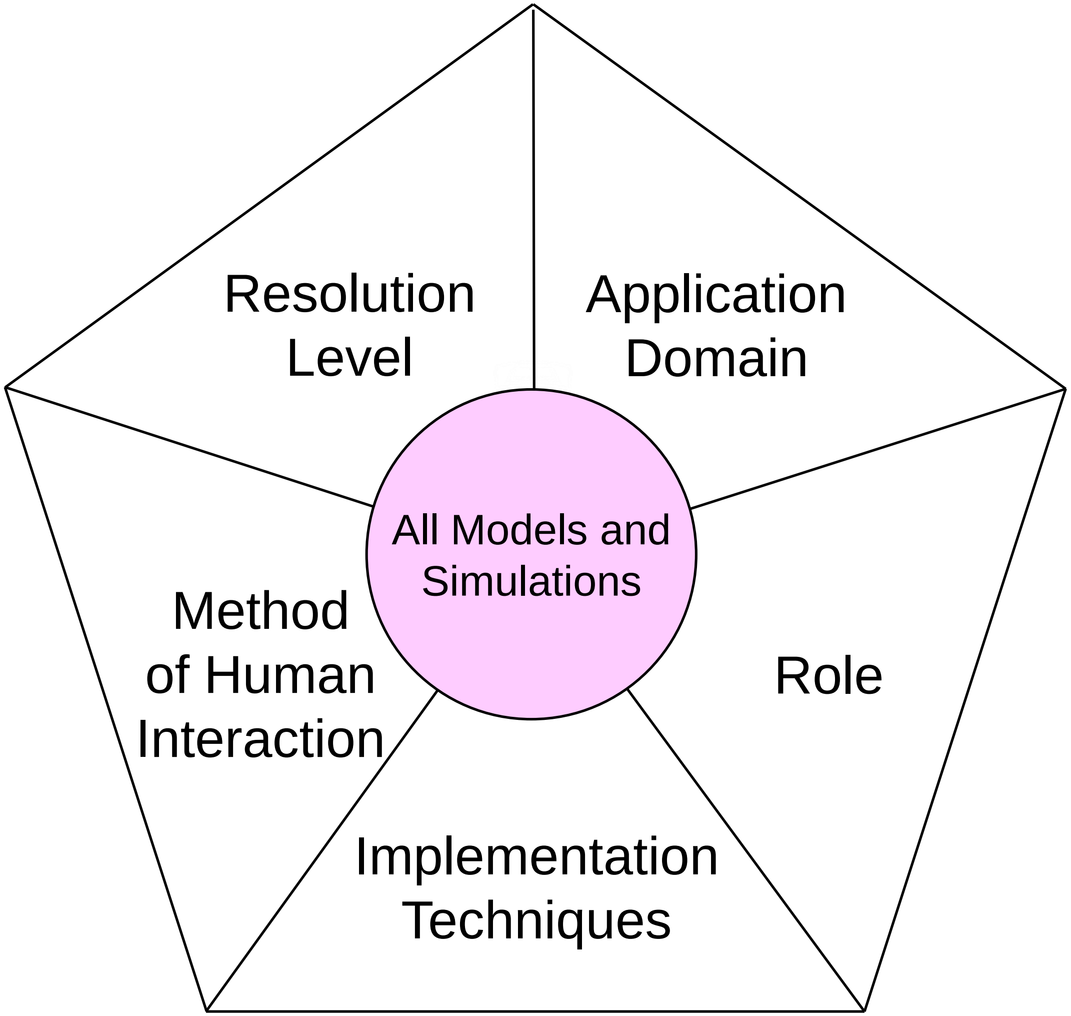
Sources: (1) Department of Defense Modeling and Simulation (M&S) Glossary, July 1, 2013; available at http://www.msco.mil/MSGlossary.html

(2) DoD 5000.59, DoD Modeling and Simulation (M&S) Management, August 2007

Distinguishing Between Models, Simulations, and M&S-Related Tools

- Models
  - Need not be computer-based
  - Represent something in the real world
  - Are “static” representations
- Simulations
  - Need not be computer-based
  - Represent something in the real world
  - Are “dynamic” representations (of models)
- M&S-Related Tools
  - Are typically computer-based
  - Do not, by themselves, represent something in the real world
  - Can be used to create (computer-based) models and simulations
- Examples
  - Microsoft Excel is a “tool” (not a model), but can be used to create a “cost model” of a system
  - AnyLogic is a modeling tool that can be used to create a “process simulation”

Five Different "Views" of Models and Simulations



Selected Major Modeling & Simulation Application Domains

- Military systems
  - Air and missile defense
  - Strike warfare
  - Undersea warfare
- Civilian systems
  - Aerospace
  - Automotive
  - Electronics
- Homeland security
  - Airborne hazard dispersion
  - Disease spread
  - Traffic evacuation
- Medicine
  - Drug discovery
  - Health care
  - Surgery simulation

Selected Major Modeling & Simulation Roles

- Planning and analysis
  - "How many of system X do I need?" "Which alternative is best?"
- Experimentation
  - "How could we use this better?" "What might happen if we tried this?"
- Systems engineering and acquisition
  - Principal focus of this course
- Test and evaluation (T&E)
  - "Does the system work as expected?" "Will it help in the real world?"
- Training
  - "How can we ensure the system is used correctly?" "How can we prepare pilots for rare emergency situations?"
- Cost estimation
  - "How much will this cost?" "How can we reduce cost?"

Modeling and Simulation Implementation Techniques

- Technique decisions to be made, based on application
  - Static vs. dynamic
  - Deterministic vs. stochastic (“Monte Carlo”)
  - Discrete vs. continuous
  - Discrete-event vs. time-stepped
  - Standalone vs. embedded (“in the loop”)
  - Unitary vs. distributed
  - Live vs. virtual vs. constructive (more to follow on next slide)
- Other technique decisions
  - Visualization needs
  - Stimulation of real systems

Categorizing Simulations by the Nature of Human-System Interaction

- ***Live*** simulation: A simulation involving real people operating real systems
  - Examples: exercises, operational tests
- ***Virtual*** simulation: A simulation involving real people operating simulated systems
  - Examples: cockpit simulator, driving simulator
- ***Constructive*** simulation: A simulation involving simulated people (or no people) operating simulated systems
  - Examples: crash test facilities, missile 6-degree-of-freedom simulations

Systems \ People	Real	Simulated
Real	Live 	?
Simulated	Virtual 	Constructive 

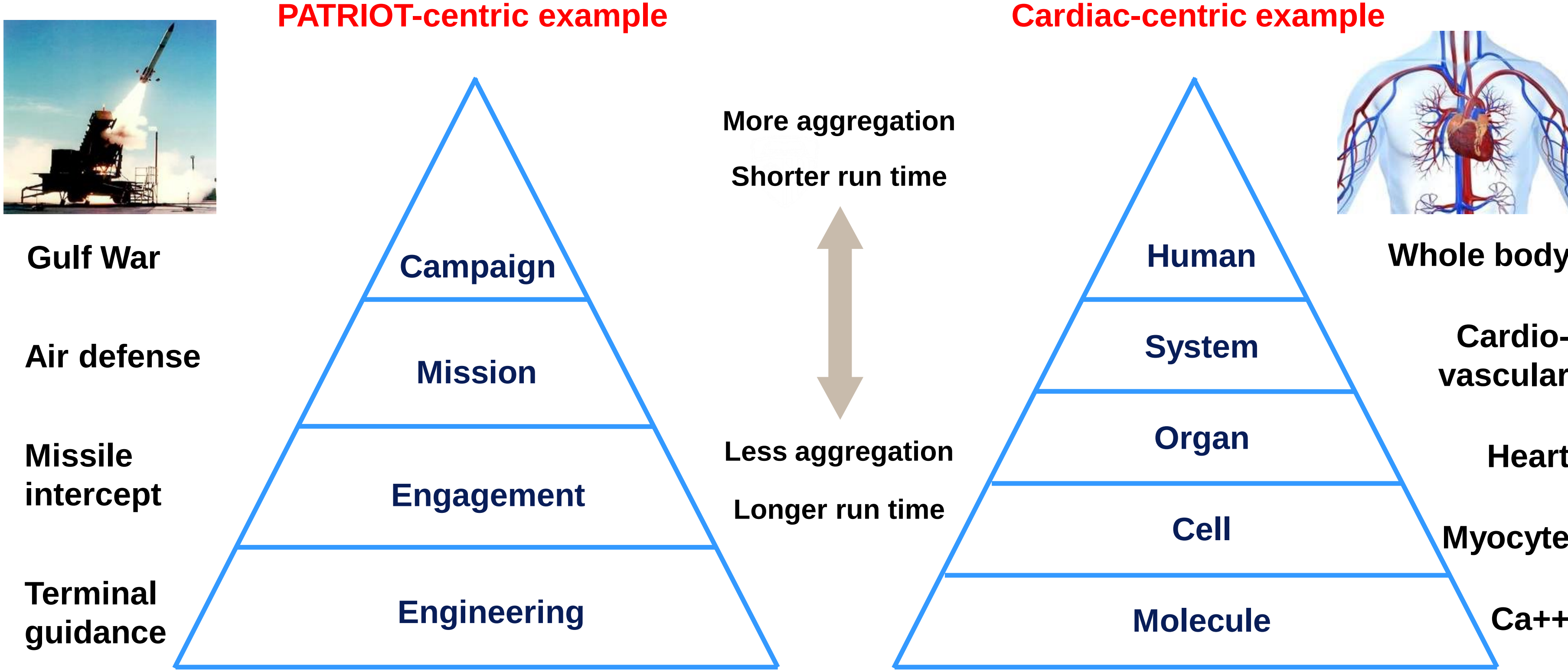
Question: What would you call a simulation involving simulated people operating real systems? If the system were an airplane, would you fly on it?

Categorizing Models and Simulations by Levels of Resolution

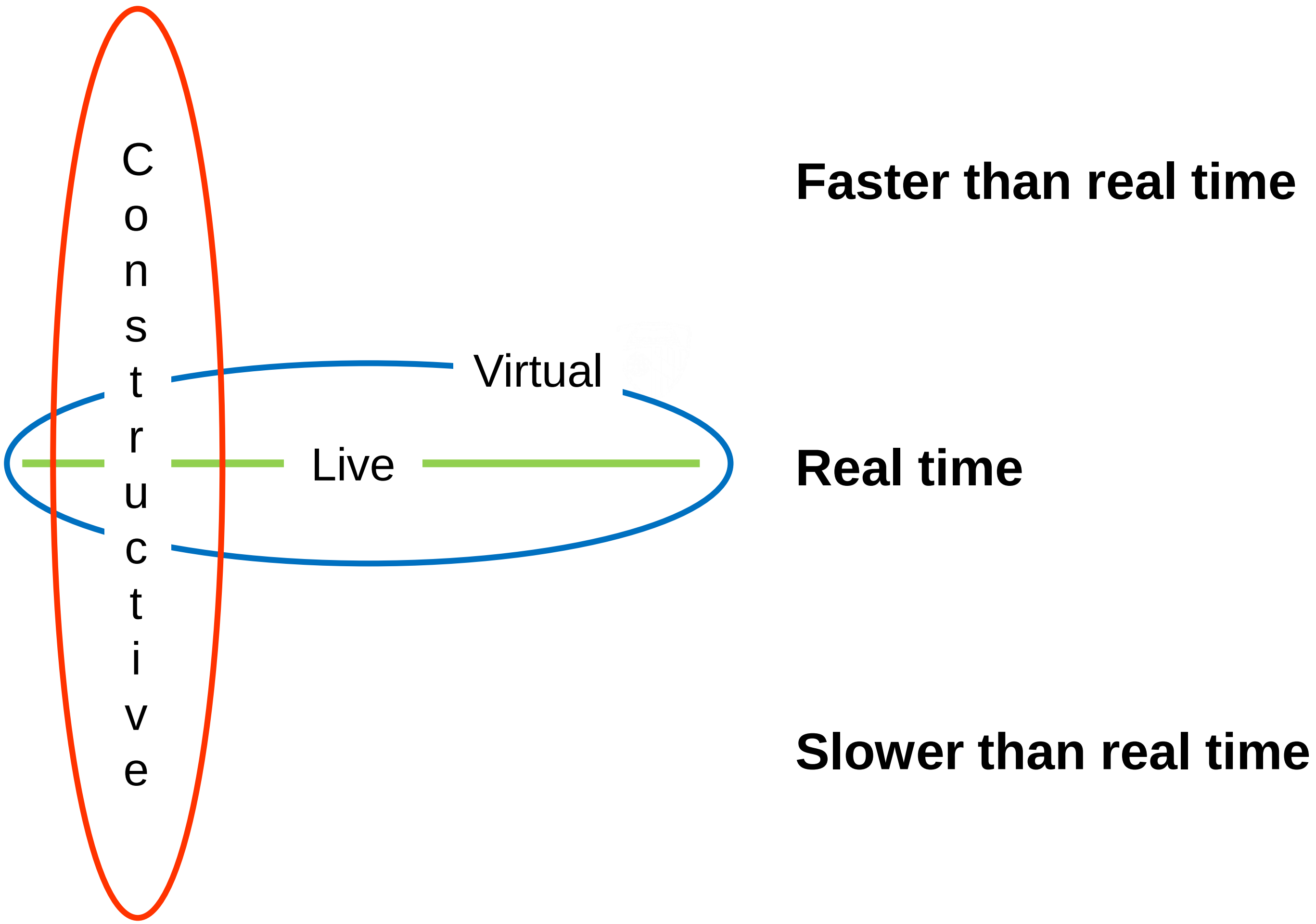
Most M&S application domains have a hierarchical means of categorizing models and simulations in that domain, by resolution level.

Military Simulation Pyramid
PATRIOT-centric example

Human Body M&S Pyramid
Cardiac-centric example



Relative Run-times of Live, Virtual, and Constructive Simulations



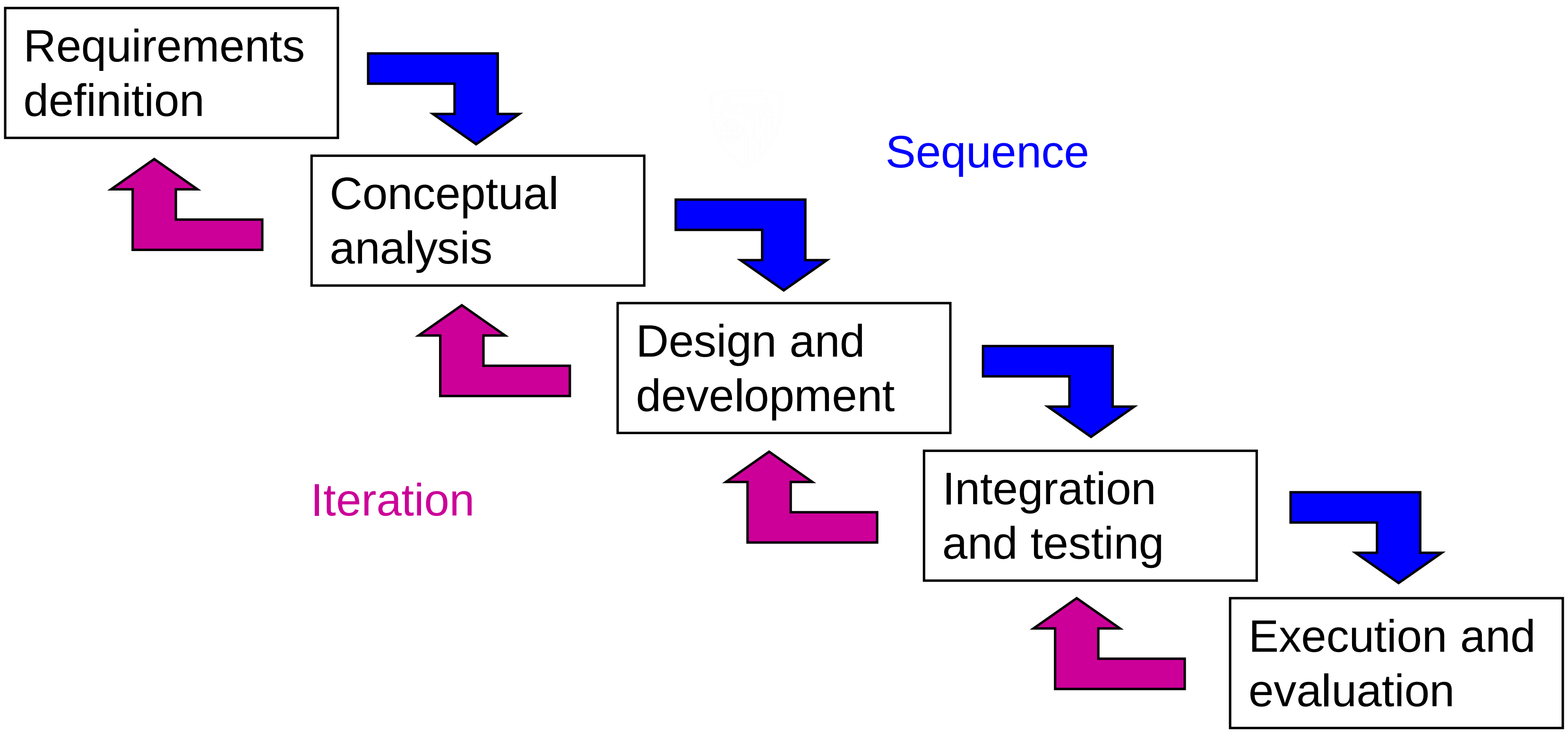
Resolution, Aggregation, and Fidelity

- Resolution: The degree of detail and precision used in the representation of real world aspects in a model or simulation
  - Models and simulations at lower levels of M&S “pyramid” tend to exhibit more resolution; this does not necessarily imply more accuracy
- Aggregation: The ability to group entities while preserving the effects of entity behavior and interaction while grouped
  - “Campaign-level” simulations often aggregate military entities into larger groups (e.g., brigades vs. battalions)
- Fidelity: The accuracy of the representation when compared to the real world
  - Greater fidelity does not imply greater resolution

Source of definitions: Department of Defense Modeling and Simulation (M&S) Glossary, July 1, 2013; available at http://www.msco.mil/MSGlossary.html

The Model/Simulation Development Process

- Developing a model or simulation is, in itself, a type of “systems engineering” process
- Although shown below as a “waterfall,” various forms of iteration are possible.



Important M&S-Related Processes: Configuration Management

- Configuration management is just as important for M&S as it is for systems and software engineering.
- Issues in model / simulation configuration management
  - Identifying the "current version" during development
  - Maintaining a copy of each "release"
  - Tracking defects and their correction
  - Maintaining records of recipients of each version
  - Managing multiple "branches" for multiple users
  - Managing co-developed versions if source is distributed
  - Incorporating externally-made changes in a "baseline" version
  - Regression testing of new versions

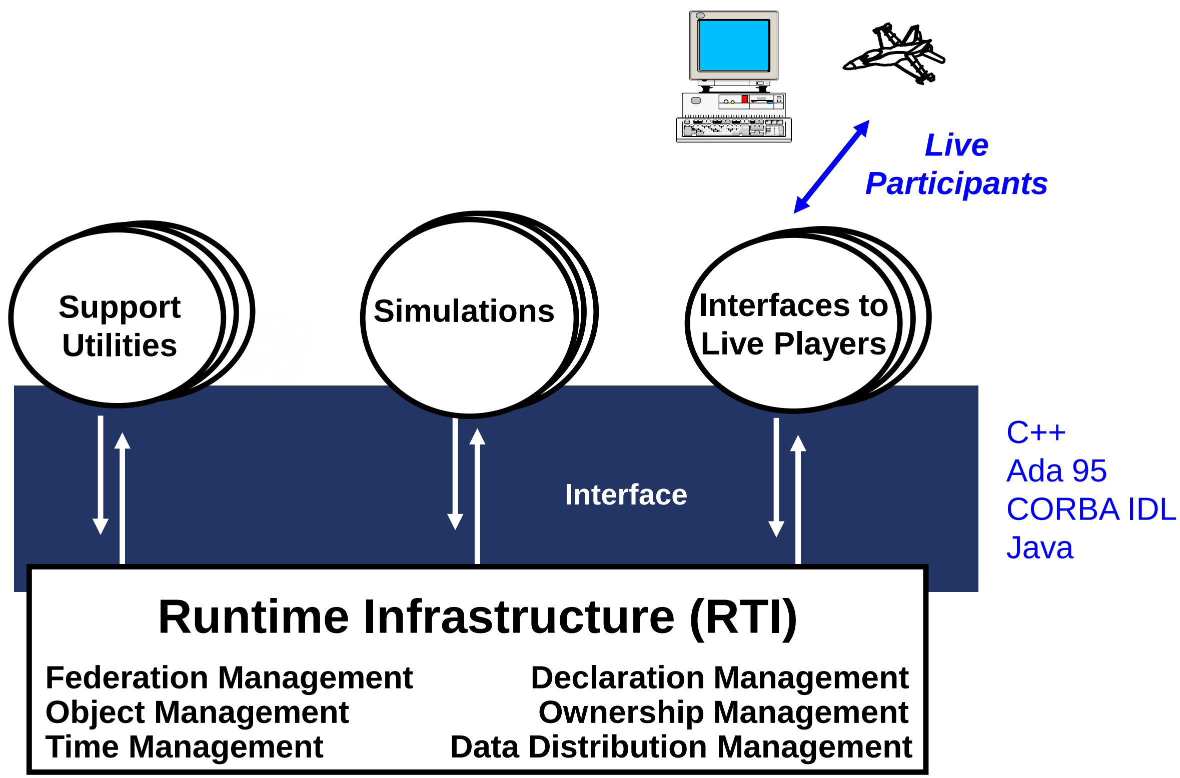
Important M&S-Related Processes: Verification, Validation, and Accreditation (VV&A)

- Verification - The process of determining that a model or simulation implementation and its associated data accurately represent the developer's conceptual description and specifications
  - *Did we build the model right?*
- Validation - The process of determining the degree to which a model or simulation and its associated data are an accurate representation of the real world from the perspective of the intended uses of the model
  - *Did we build the right model?*
- Accreditation - The official certification that a model or simulation and its associated data are acceptable for use for a specific purpose
  - *Is this the right model to use for this purpose?*

Source: DoD Instruction (DoDI) 5000.61 DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A), December 9, 2009

Interoperable Simulation: The High Level Architecture (HLA)

- Architecture calls for a federation of simulations
- Architecture specifies
  - Ten Rules that define relationships among federation components
  - An Object Model Template that specifies the form in which simulation elements are described
  - An Interface Specification that describes the way simulations interact during operation



The HLA was originally developed by DoD. It is now IEEE standard 1516.

Modeling and Simulation as an Academic Discipline

- Very few Universities offer Modeling & Simulation as an academic discipline with a degree program
- Graduate-level M&S degree programs are offered in the U.S. by:
  - The University of Central Florida (UCF)
  - Old Dominion University (ODU)
  - The University of Alabama in Huntsville (UAH)
  - The Naval Postgraduate School (NPS)
  - Arizona State University (ASU)
  - Purdue University Calumet
  - Philadelphia University
- M.S. degree concentrations in M&S are offered by:
  - The Johns Hopkins University (JHU) [in Systems Engineering]
  - Columbus State University (GA) [in Applied Computer Science]

Modeling and Simulation as a Professional Discipline

- Professional certification in M&S is available
  - Certified Modeling and Simulation Professional (CMSP) designation
    - Originated by the National Training and Simulation Association (NTSA)
    - Now administered by the Modeling and Simulation Professional Certification Commission (M&SPCC)
  - Requirements:
    - Relevant (simulation) work experience and educational requirements, three letters of recommendation, and a passing grade on the exam
    - Fee of $250
    - 14 days allowed to answer 100-question examination
  - See web site: http://www.simprofessional.org

Module Summary

- A model is a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. A simulation is a method for implementing a model over time.
- Models and simulations can be categorized by their application domain, role, implementation techniques, method of human interaction, and level of resolution.
- Developing a model or simulation is, in itself, a type of systems engineering process.
- Configuration management and VV&A are two important M&S processes.
- Simulations may be made to interoperate with one another using various techniques, including the HLA (IEEE 1516).
- M&S has not completely emerged as a separate academic discipline, but is beginning to be recognized as a professional discipline.

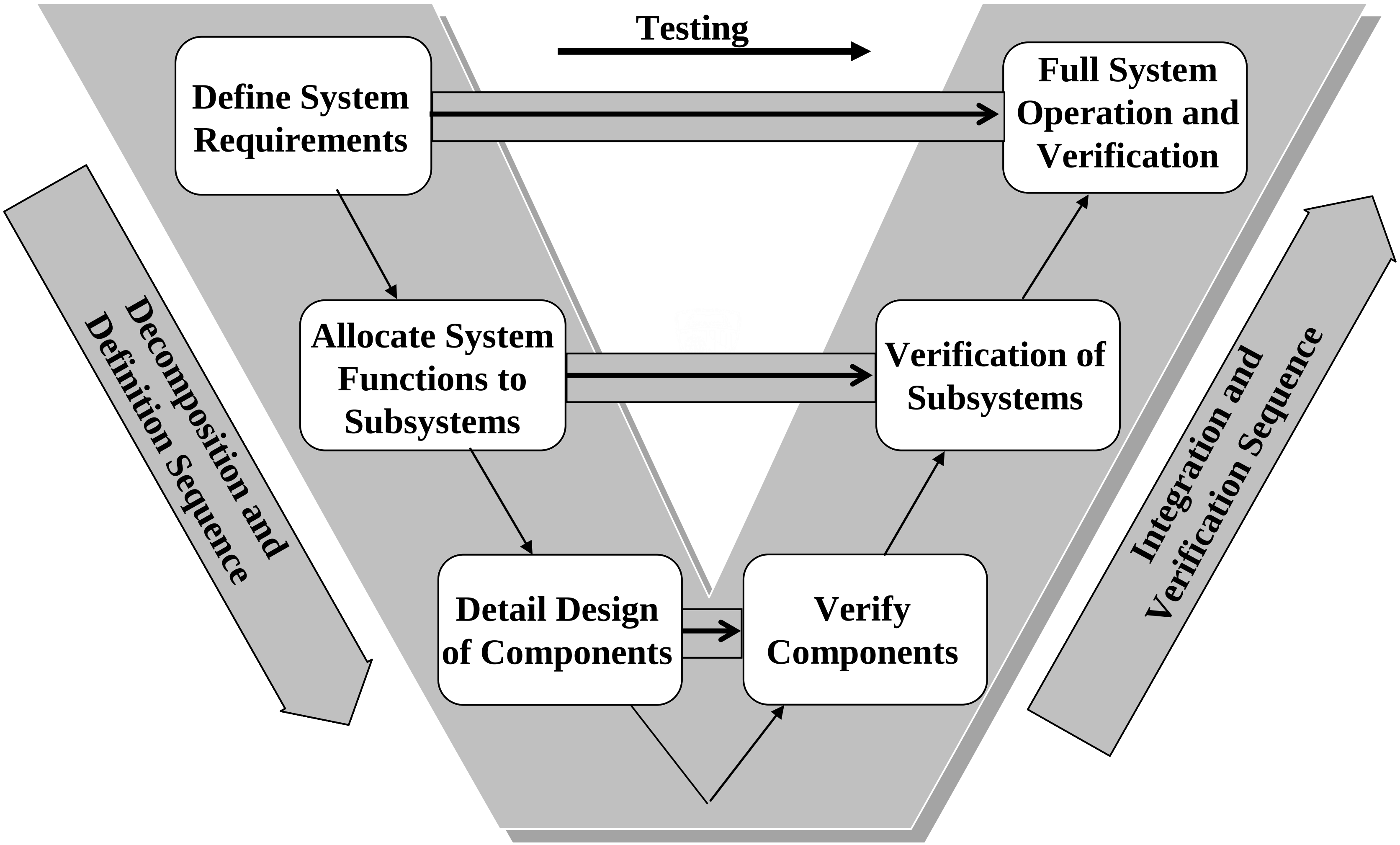
Coolahan Associates, LLC™

JOHNS HOPKINS WHITING SCHOOL of ENGINEERING

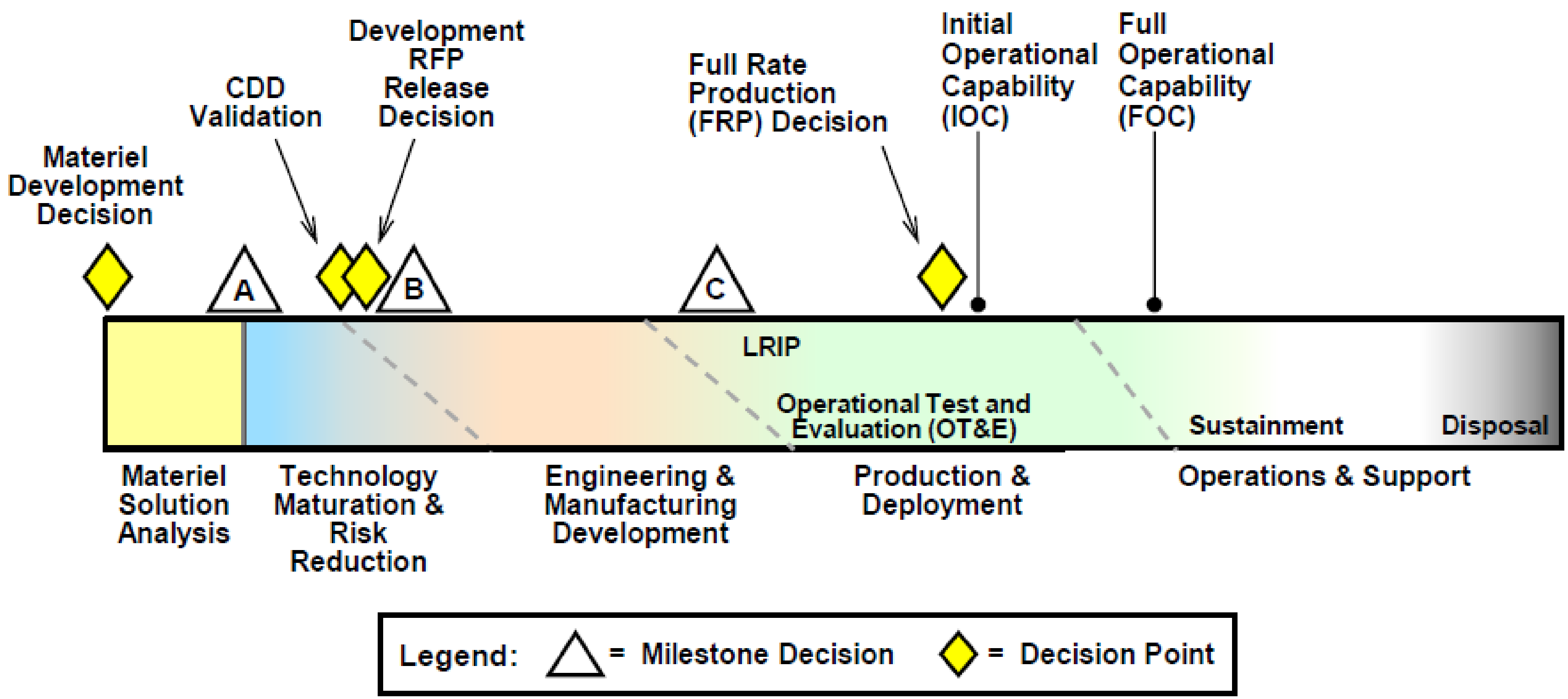
Part 2:
Use of M&S by Phase of the Systems Engineering Process

Systems Engineering Process Model for This Tutorial

The “V” Model of Systems Engineering



Defense Acquisition Program Model
(for Hardware-Intensive Program)



Five other variants of this program model exist for other types of programs.

Source: DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015

A Representative Six-Stage System Life Cycle

Concept stage	**Development stage**	**Production stage**	**Utilization stage**	**Support stage**	**Retirement stage**

Source: ISO/IEC TR 19760, *Systems engineering — A guide for the application of ISO/IEC 15288 (System life cycle processes)*, 2003

A Textbook Representation of Systems Engineering Stages & Phases

Systems Engineering Stages	**Concept Development**			**Engineering Development**			**Post Development**	
Systems Engineering Phases	Needs Analysis	Concept Exploration	Concept Definition	Advanced Development	Engineering Design	Integration & Evaluation	Production	Operations & Support

Source: *Systems Engineering: Principles and Practice*, Kossiakoff, A., Sweet, W. N., Seymour, S. J., and Biemer, S. M., Wiley, 2011.

A Reference Model of the Systems Engineering Process for this Tutorial

- **System Needs and Opportunities Analysis**
  - Defining and validating needs, and determining feasibility
- **Concept Exploration and Evaluation**
  - Exploring and evaluating system concepts, refining required performance characteristics and required effectiveness in representative operational environments, and performing analysis of alternative concepts
- **Design and Development**
  - Designing and prototyping the system, providing for human-system integration, refining performance estimates, and production planning
- **Integration and Test & Evaluation (T&E)**
  - Integrating the system components, and testing/evaluating the system in representative environments
- **Production and Sustainment**
  - Producing and sustaining the system, including providing for reliability, availability, logistics, and training

Comparison of System Life Cycle Models

<table>
<tr><td>DOD 5000.02 (Hardware-Intensive Systems), 2015</td><td>Materiel Solution Analysis</td><td colspan="2">Technology Maturation & Risk Reduction</td><td colspan="3">Engineering & Manufacturing Development</td><td>Production & Deployment</td><td colspan="3">Operations & Support</td></tr>
<tr><td>ISO / IEC 15288, 2003</td><td>Concept</td><td colspan="5">Development</td><td>Production</td><td>Utiliza-tion</td><td>Support</td><td>Retire-ment</td></tr>
<tr><td>Kossiakoff Textbook (Stages), 2011</td><td colspan="3">Concept Development</td><td colspan="3">Engineering Development</td><td colspan="4">Post-Development</td></tr>
<tr><td>Kossiakoff Textbook (Phases), 2011</td><td>Needs Analysis</td><td>Concept Exploration</td><td>Concept Definition</td><td>Advanced Develop-ment</td><td>Engineering Design</td><td>Integration & Evaluation</td><td>Production</td><td colspan="3">Operations & Support</td></tr>
<tr><td>This Course</td><td>System Needs & Opportu-nities Analysis</td><td colspan="2">Concept Exploration & Evaluation</td><td colspan="2">Design & Development</td><td>Integration and Test & Evaluation</td><td colspan="4">Production & Sustainment</td></tr>
</table>

Coolahan Associates, LLC™

JOHNS HOPKINS WHITING SCHOOL of ENGINEERING

Modeling and Simulation in System Needs and Opportunities Analysis

Module Objectives and Outline

Module Objective:

- To describe the use of modeling and simulation in the system needs and opportunities analysis phase of the systems engineering process.

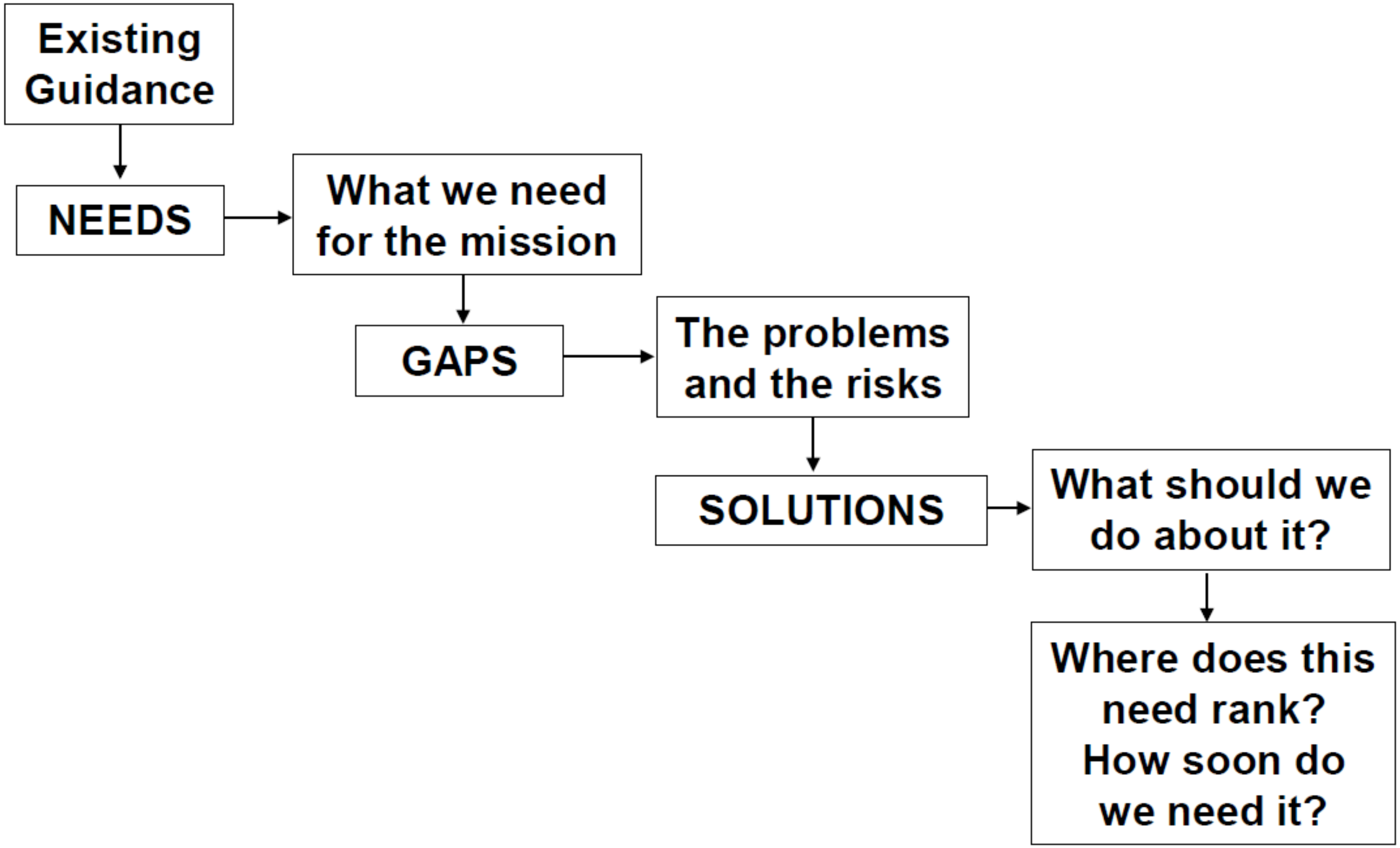
Module Outline

- Needs vs. Opportunities for New or Improved Systems
- The U.S. Military Process for Capabilities-Based Assessment
- Commercial System Processes
- M&S Use in Operational Analysis
- M&S Use in Functional Analysis
- M&S Use in Feasibility Determination
- Summary

Needs vs. Opportunities for New or Improved Systems

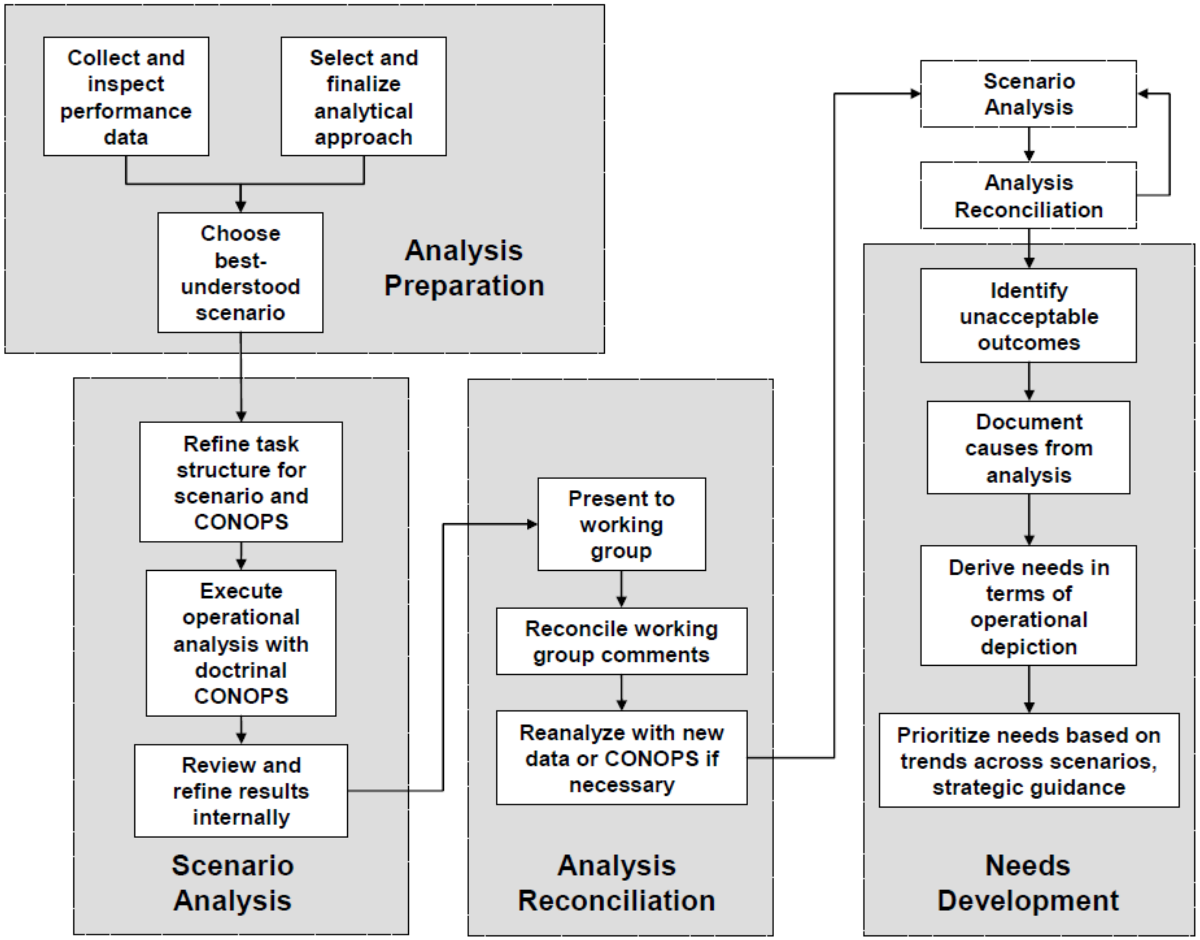
- New or improved systems can be initiated
  - As the result of the *need* for a new or improved capability; or
  - To take advantage of an *opportunity*
- For military systems
  - A need can result from the emergence of a new threat
  - An opportunity can arise because of a technology breakthrough
- For commercial systems
  - A need can result from a new legal or regulatory requirement
  - An opportunity can arise from a new demand in the marketplace or financial incentives to provide an improved capability (e.g., hybrid autos)
- M&S can be used to
  - Explore the effectiveness or utility of a new concept
  - Estimate the cost of envisioned alternatives
  - Aid in determining feasibility of a new or improved system

Capabilities-Based Assessment (CBA) Process in the U.S. Joint Capabilities Integration and Development System



Source: Joint Capabilities Integration and Development System (JCIDS) – A Primer

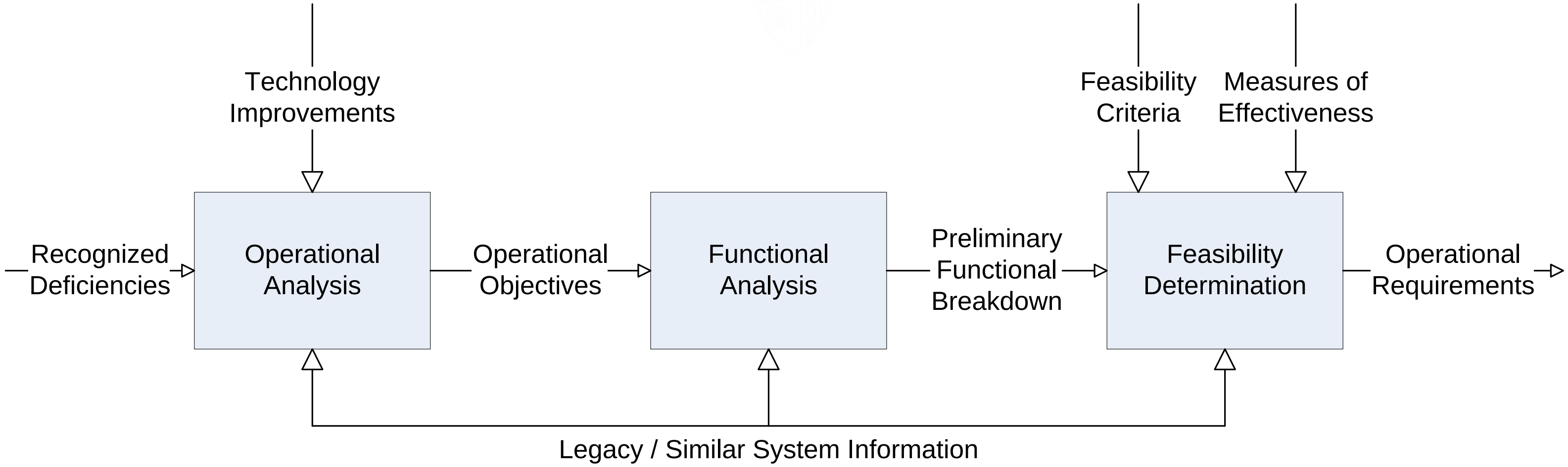
Capabilities-Based Assessment Needs Assessment Task Flow



Source: Capabilities-Based Assessment (CBA) User's Guide

Commercial Processes for Identifying and Analyzing Needs and Opportunities

- Commercial processes can vary depending on the industry and the individual company
- In general, there is a fairly continual *operational analysis* process, which periodically triggers a *functional analysis* based on a set of operational objectives, followed by a *feasibility determination* resulting in operational requirements for a new or improved system



Simplified Needs and Opportunities Analysis Diagram

Modeling and Simulation Use in Operational Analysis (1 of 3)

- Simulations of (Relative) Performance
  - Although the absolute performance of a system will generally not decrease over time (and will often increase through upgrades), its *relative* performance eventually degrades
    - A new missile threat may have capabilities outside the performance envelope of an air defense system
    - Competing products may incorporate new technology (e.g., cell phone decreasing size and weight, longer battery life)
  - Simulations of the threat or competitive *environment* must be continually executed to predict system obsolescence

Modeling and Simulation Use in Operational Analysis (2 of 3)

- Models of Total Ownership Cost
  - Changing costs for operations and maintenance labor or consumables may impact how much a user must pay to own the product
    - At certain thresholds of the price of gasoline, ownership of vehicles with higher gasoline consumption can become unaffordable
  - Models of *all* ownership costs must be developed and maintained
- Models of Sustainability
  - At some point in time, parts for a given system implementation may no longer be available, at any cost
  - Models of parts availability must be developed and maintained

Modeling and Simulation Use in Operational Analysis (3 of 3)

- Value Modeling Tools
  - Some value attributes of systems defy quantitative engineering measurement
    - "Intelligence estimates" of the performance and fielding date of future threats are dependent on judgment of subject matter experts (SMEs)
    - "Stylishness" of new cars is in the eyes of the beholders
  - Models of value using multiple unrelated measures need to be constructed
    - Value attributes must be identified
    - Measures for collecting valid opinions and quantifying them must be devised
    - A "weighting scheme" must be applied in the model

Illustration of M&S Use in Operational Analysis

- Simulation of System Operations through Games
  - Can be a structured “war game” with blue, red, white, green cells
  - Can be a “seminar” game with subject matter experts in various fields working collaboratively
  - Can be used to explore concepts of operations for proposed systems
  - The term “serious games” has come into vogue to describe these

Seminar Game Example:

- *How would I use the existing system in this scenario?*
- *What technology improvements could be made?*
- *If I had a system with this capability, what would I do now in this situation?*

Modeling and Simulation Use in Functional Analysis

- Functional analysis needs to translate operational system objectives into system functions
  - Essentially, a feasible concept must be able to be "envisioned"
  - In a need-driven process, some system functions might be relatively well-known from legacy systems
- Deriving a functional structure contains elements of art / architecting
- Modeling tools can be used to develop a system functional breakdown
  - Can start with a relatively simple block diagram (e.g., Microsoft Visio or PowerPoint could be used to generate a top-level "model" of a system)
  - More formal notations can be used to ensure inputs and outputs are properly considered (e.g., IDEF0 diagrams or Unified Modeling Language (UML) diagrams)

Modeling and Simulation Use in Feasibility Determination (1 of 3)

- Simulations of System Operational Effectiveness – Input Needs
  - Estimates of the performance of an envisioned system implementation, at a less-detailed level, such as
    - Probability of detection as a function of target cross-section and range (in various environments) for a radar system
    - Miles per gallon as a function of fuel octane, temperature, and pressure for an automobile
  - Similar estimates for systems with which the envisioned system must interact collaboratively or cooperatively
  - For systems with competitive adversary systems, similar estimates for each adversary system
  - Representations of the natural environment (land, sea, and/or air), often time-varying
  - A model of one or more representative scenarios of use of the system, including such things as geographic location, environmental conditions, time of day, system behaviors, etc.

Modeling and Simulation Use in Feasibility Determination (2 of 3)

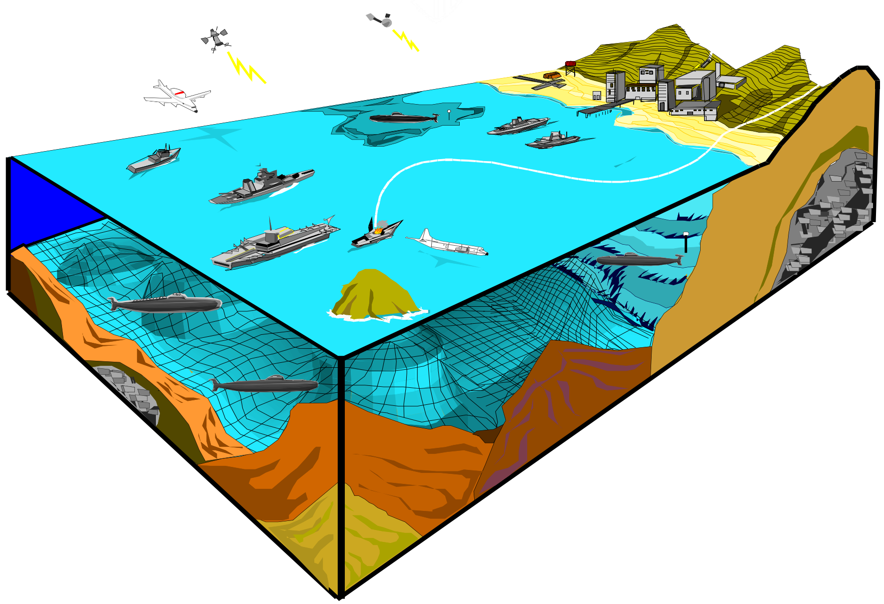
- Models of Total Ownership Cost
  - Similar to those used during operational analysis
- Models of Sustainability
  - Reliability models (at a relatively high level, unless data on similar legacy system components are available)
  - Availability models (percentage of time the system will be ready when called upon)
  - Maintainability models (e.g., time to repair)
  - Logistics support simulations

Modeling and Simulation Use in Feasibility Determination (3 of 3)

- For systems that are improvements to existing systems and/or use legacy components, models and simulations of those systems / components can be used as a starting point
- The outputs of models and simulations in the feasibility determination phase are generally various estimated *measures of effectiveness* for a particular envisioned system implementation

Illustration of M&S Use in Feasibility Determination

- Campaign-level Simulations
  - Use Measures of Performance (MoPs) of systems as inputs
  - Simulate system operation in a computer-based operational environment
  - Produce Measures of Effectiveness (MoEs) as outputs
  - Can be used to answer “so what” questions for proposed new systems



Module Summary

- New or improved systems can be initiated as the result of the need for a new or improved capability, or to take advantage of an opportunity
- For both military capabilities and commercial systems, there are somewhat similar approaches to needs/opportunities analysis, but using different terminology
- Value modeling tools are often useful during operational analysis to help quantify SME opinions
- Formal modeling notations and tools are useful in adding rigor to system functional breakdowns
- Operational effectiveness simulations are important in performing
  - Ongoing operational analysis to determine operational objectives for new or improved systems
  - Analysis of envisioned system implementations to determine feasibility
- Cost models must consider the total ownership cost of systems, not just the development cost
- Sustainability (reliability, availability, maintainability, logistics) models and simulations are also of significant importance in operational analysis and feasibility determination

Modeling and Simulation in Concept Exploration and Evaluation

Module Objective and Outline

Module Objective: To describe the use of modeling and simulation in the concept exploration and evaluation phase of the systems engineering process.

Module Outline

- Scope of Concept Exploration and Evaluation
- A Simplified Process Model for Concept Exploration and Evaluation
- Effectiveness Simulations
  - Components of Effectiveness Simulations
- Analyses of Alternatives
  - System Effectiveness Simulation
  - Cost Modeling
- Ensuring a “Level Playing Field”
- Summary

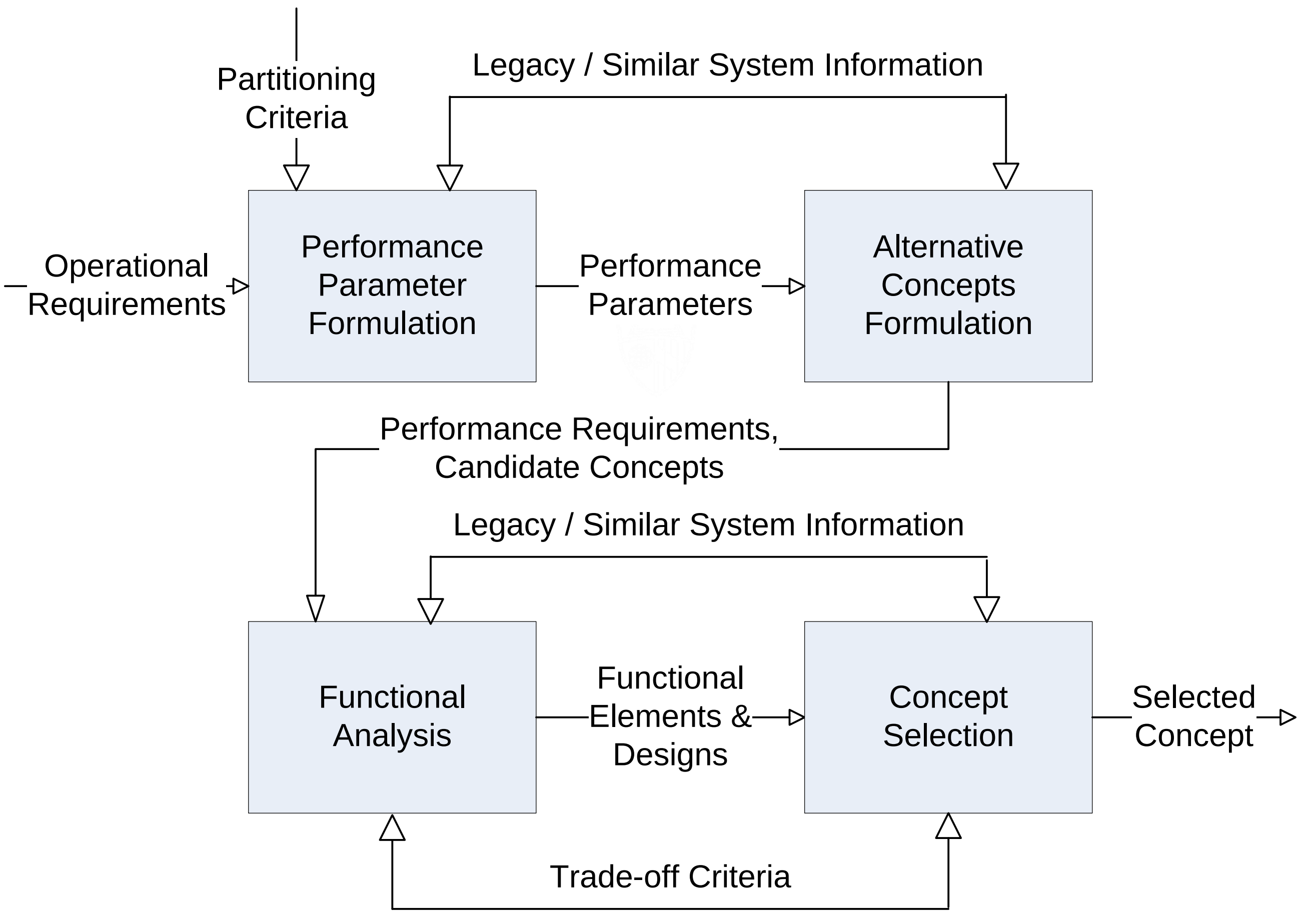
Scope of Concept Exploration and Evaluation (1 of 2)

- **Concept Exploration**
  - Involves translating the operational requirements for the system into engineering-oriented *performance requirements* for the system
    - interpret, but do not replace, the operational requirements
  - Several alternative candidate system concepts are envisioned, and their performance characteristics established
  - Can sometimes be relatively limited, to only particular functions or portions of a legacy system
  - For new systems, a more creative, non-prescriptive method is indicated that is akin to *systems architecting*

Scope of Concept Exploration and Evaluation (2 of 2)

- **Concept Evaluation**
  - Involves taking the alternative concepts produced during concept exploration, defining them even further, and evaluating them
  - May be done by a single organization or, in the case of a major system development by separate organizations in a competitive environment, with an independent organization evaluating those concepts
  - Results in a selected system concept and a set of system functional specifications suitable to enter development

A Simplified Process Model for Concept Exploration and Evaluation



Use of Legacy / Similar System Information and M&S Tools

- Reuse of models/simulations is usually cost-effective
  - Usually require some adaptation
  - Need subject matter experts & M&S professionals familiar with tools
  - Less experienced teams can make use of M&S repositories / registries to assist in discovery process
- Issues to be aware of
  - Lack of awareness of existing M&S tools
  - “Not invented here” (NIH) syndrome
  - Force-fit of familiar tools (“we’ve always used this one”)
- Best to do selection based on objective set of requirements / criteria
- Availability of authoritative data can be an issue
  - Authoritative data on military threat systems may be hard to obtain
  - Authoritative data on “friendly” systems may require time-consuming release approval

Effectiveness Simulations

- Effectiveness simulations – typically at the “mission level” of the military simulation pyramid
- Generally use parameterized system performance data generated by performance simulations
- Major components of effectiveness simulations
  - The system representation (in performance terms)
  - The system’s concept of operations
  - The representation of threats and friendly systems
  - The representation of the natural and man-made environment
  - The scenario
- Supporting elements of effectiveness simulations
  - User interface
  - Data input mechanisms
  - Results output mechanisms

Effectiveness Simulations – Representing the System

- During concept exploration and evaluation
  - Only early estimates of system performance may be available
  - Systems based on legacy components typically have more credible representations than those based on new technology
- Can sometimes use effectiveness simulations for screening
  - "If we could build a system with this performance, would it make a difference?"
  - Does achieving desired performance require unrealistic operational conditions?
- System performance typically represented parametrically
  - Using equations
  - Using tables of two or more dimensions

Effectiveness Simulations – Concept of Operations

- Need to represent how the system is employed in practice
  - Concept of operations (CONOPS) can affect system performance
- Examples of CONOPS effects on performance
  - Submarine towed array system performance affected by dynamic movement during submarine maneuvers
  - Ground-based system may not be activated until cued by a surveillance system
  - Automotive system may only be activated when commanded by the driver
  - Flight performance of aircraft affected by formation flying
    - Why do ducks fly in a V formation?

Effectiveness Simulations – Threats and Friendly Systems

- Virtually every system, whether commercial or military, will need to interact with other systems
  - Need to represent other systems to the degree that their performance could impact the system’s effectiveness
  - For commercial systems, most are cooperative, or at least neutral
  - For military systems, must take into account the performance of:
    - Threat (“red”) systems
    - Cooperating (friendly, or “blue”) systems
    - Neutral (“green”) systems (important in “irregular warfare”)
- Level of detail at which such systems need to be represented depends on nature of potential interactions with system being studied
  - If neutral systems are only “clutter,” can be modeled simply
  - Some cooperative systems may only need to be modeled as a source of communication messages, with a probability of successful delivery
  - But some threat systems need detail commensurate with system being studied (e.g., threat aircraft in a “dogfight” scenario)

Effectiveness Simulations – The Natural and Man-Made Environment (1 of 2)

- The effectiveness of virtually all systems is dependent on the effects of the natural and the man-made environments that it encounters during operation
  - Some effects are well known and tolerable (e.g., automobile radio or Global Positioning System (GPS) reception in middle of two-mile tunnel; cell phone performance in urban canyons)
  - Some effects are not tolerable (e.g., automobile engine overheating in Death Valley)
- Environmental conditions are typically more important for military (and law enforcement, and other government) systems, which are needed to operate with high reliability in more stressful environments than commercial systems
  - Dust storms for ground vehicles, jamming environments for communication systems, and supersonic airflows for aircraft
  - In other cases, some degradation of performance can be tolerated, but needs to be quantified (e.g., sonar performance)
- Effectiveness simulations must model environmental conditions with fidelity commensurate with their effects on the system.

Effectiveness Simulations – The Natural and Man-Made Environment (2 of 2)

- Models of the natural environment include
  - Atmospheric characteristics, such as temperature, pressure, humidity, and wind speed – for airborne systems and electromagnetic propagation
  - Ground terrain characteristics, such as height vs. position and soil properties – for ground-based systems and line-of-sight calculations
  - Ocean characteristics, such as depth, sound velocity profile, and wave height – for maritime systems
  - Space characteristics, such as solar flares and sun spots – for satellite reliability/availability and electromagnetic propagation.
- Models of the man-made environment include
  - Building sizes and shapes – for line-of-sight calculations, and urban wind velocity / contaminant propagation
  - Road networks – for transportation modeling
  - Electromagnetic emissions – for electromagnetic interference calculations

Effectiveness Simulations – Scenarios

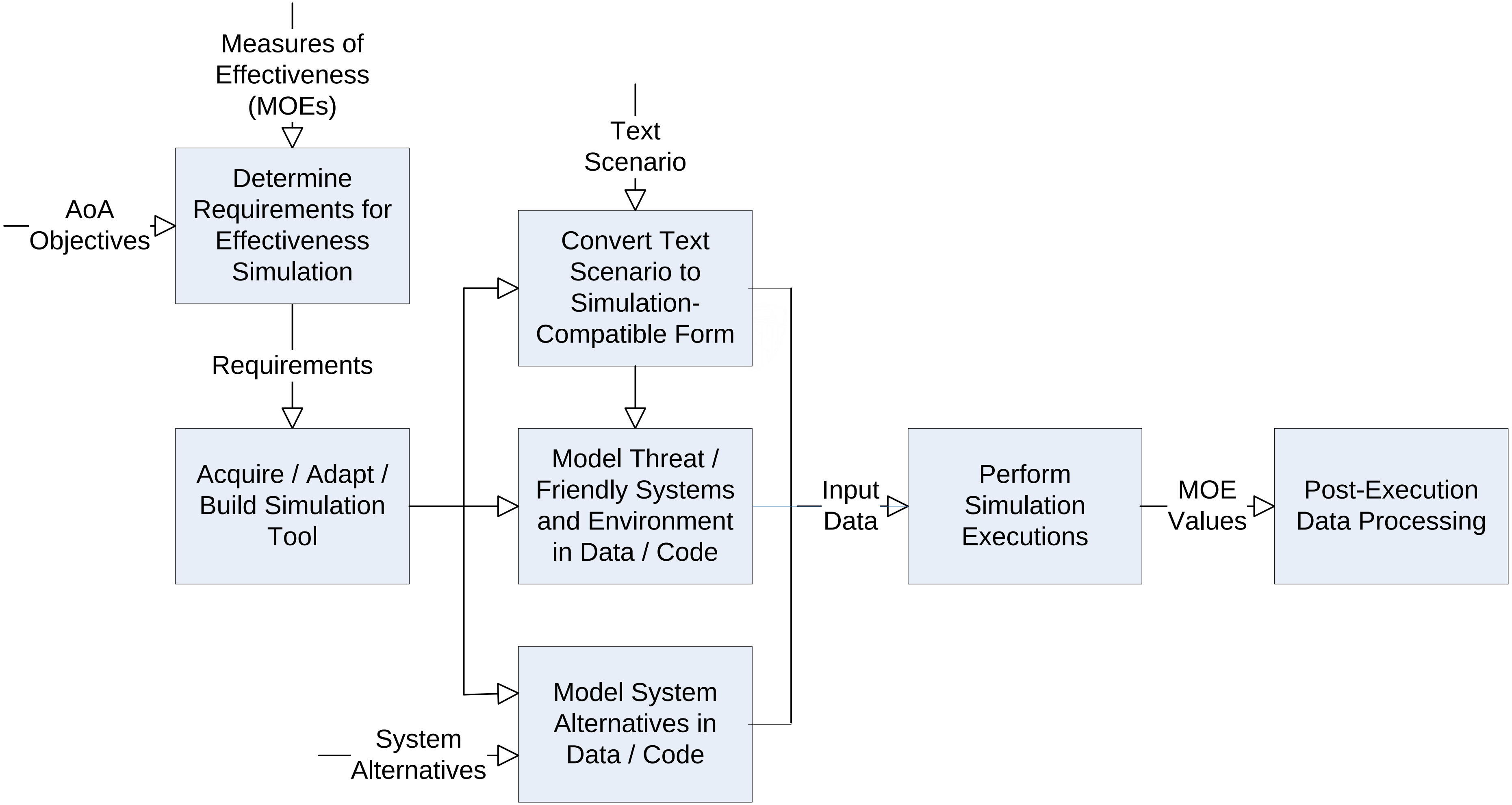
- Scenarios often start out as high-level text descriptions
  - But must be quantified to be used in effectiveness simulations
- Scenarios for a military simulation will typically include
  - The numbers and types of each friendly, threat, and neutral system involved
  - System concepts of operation, and the way in which entities move (either scripted, or in some reactive way)
  - Location and extent of the “play box(es)”
  - Instantiations of the natural and/or man-made environment, sometimes in great detail (e.g., Digital Terrain Elevation Data (DTED) terrain files)
  - A time of year (important for choosing appropriate atmospheric and maritime data)
  - A duration, which could range from as little as seconds for a missile intercept to days or weeks for an extended ground battle

Analyses of Alternatives

- An Analysis of Alternatives (AoA) is an analytical comparison of the operational effectiveness, suitability, and life-cycle cost (or total ownership cost, if applicable) of alternatives that satisfy established capability needs.
- Involves performing
  - Selection of alternatives
  - Determination of effectiveness measures
  - Effectiveness analysis
  - Cost analysis
  - Cost-effectiveness comparisons

Relationship of AoAs to the Defense Acquisition Process
Source: Defense Acquisition Guidebook

Analyses of Alternatives – System Effectiveness Simulation



Analyses of Alternatives – Cost Modeling

- Need to consider all elements of system cost:
  - Development cost
  - Production cost
  - Support (repairs, logistics, training, etc.) cost
  - Disposal cost
- Development cost modeling
  - Need to assess development risk, cost uncertainty
- Production cost modeling
  - Need to account for manufacturing systems development cost, number of units
- Support cost modeling
  - Support cost is usually the largest element of total cost (~50%)
  - Need to consider life of system, number of operators, logistics system
- Disposal cost modeling
  - Often neglected; need to consider hazardous materials

Analyses of Alternatives – Ensuring a “Level Playing Field”

- When comparing system alternatives, need to ensure that each system is modeled “fairly” with respect to other systems
- Need to model systems themselves at similar levels of resolution
- Need to take into account key concepts of operation for each system
  - For example, energy management for some radar systems
- Need to model aspects of environment at appropriate levels of detail
  - For example, line of sight for ground-based weapon systems

Module Summary

- Concept exploration and evaluation devises and evaluates a number of alternative system concepts
- Reuse of existing models and system effectiveness simulation tools, and of data on legacy systems, can often be useful in this phase
- Effectiveness simulations include
  - The system representation (in performance terms)
  - The system's concept of operations
  - Representations of threats, friendly systems, and the natural and man-made environment
  - Scenarios of system use
- An analysis of alternatives (AoA) is typically performed for major defense systems, and employs both system effectiveness simulations and cost models
- When used to compare the effectiveness of alternative systems, simulations must ensure a "level playing field" for all of the systems

Coolahan Associates, LLC ™

JOHNS HOPKINS
WHITING SCHOOL of ENGINEERING

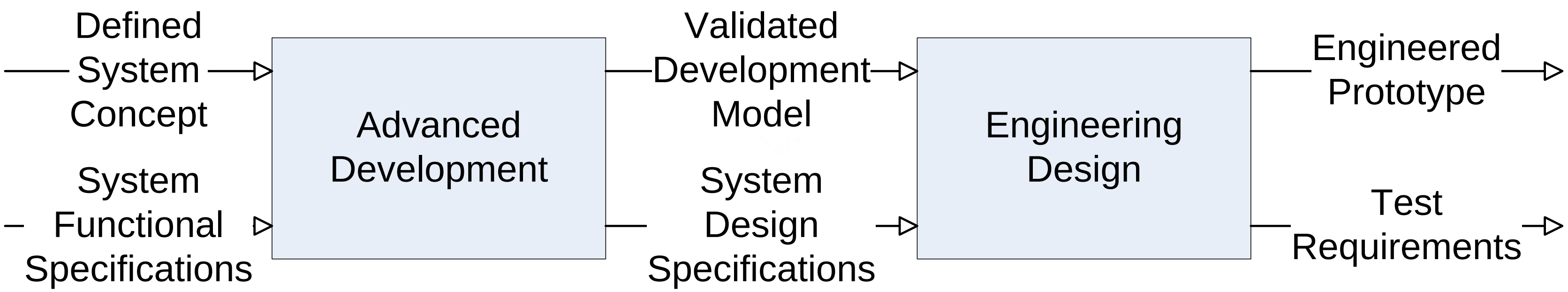
Modeling and Simulation in Design and Development

Scope of Design and Development

- The design and development phase of systems engineering, as discussed in this course, refers to the combination of the following in *Systems Engineering: Principles and Practice* [1]:
  - Advanced Development
  - Engineering Design
- Design and development takes a system concept as input, and transforms it into a set of realized system components that are ready for system integration and testing

Source: (1) Kossiakoff, A., Sweet, W. N., Seymour, S. J., and Biemer, S. N., *Systems Engineering: Principles and Practice, Second Edition*, John Wiley & Sons, Inc., Hoboken, N. J. (2011).

A Simplified Process Model for Design and Development



Distinguishing Characteristics of M&S Use in Design and Development

- Most of the simulations used during design and development fall within the “engineering” level of the four-level (military) simulation pyramid
  - They usually model individual components of the system
  - They often execute slower (or much slower) than real time
  - In many cases, they need to interface with one another to represent a subsystem or the system as a whole
  - They produce data useful as input for engagement-level simulations
- Whereas the earlier phases of the systems engineering process may utilize a relatively small number of models and simulations, in Design and Development, there is typically a large number of rather diverse models and simulations that are employed.
- Just as a systems engineer typically needs broad expertise to “ask the right questions” across a range of engineering disciplines during Design and Development, a systems engineer responsible for M&S needs to have a broad view of M&S tools that can be applied in a range of disciplines during this phase.

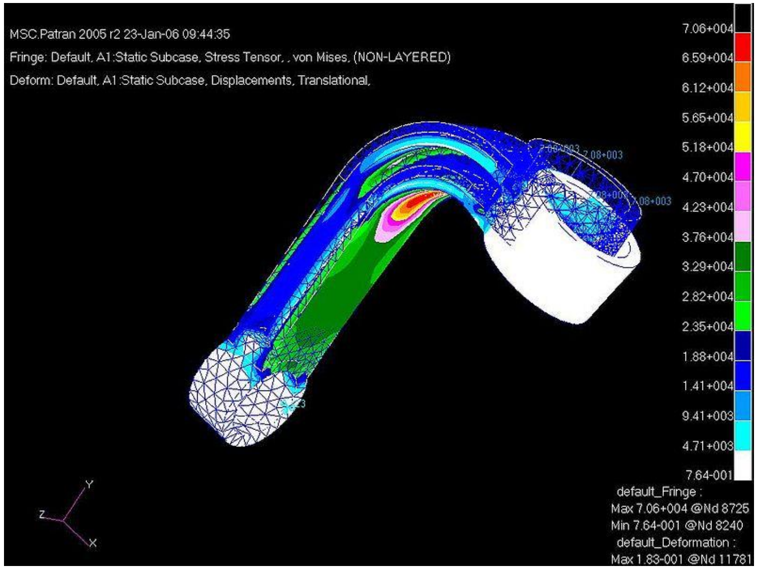
Range of Engineering Disciplines Needed for System Design and Development Simulations

- Structural mechanics/dynamics
- Fluid dynamics
- Thermal analysis
- Propulsion
- Materials engineering
- Printed circuit design
- Electrical power system design
- Guidance, navigation and control
- Communication systems engineering
- Computer network engineering
- Acoustic propagation
- Electromagnetic propagation
- Optical systems engineering
- Software engineering
- Manufacturing process modeling
- Cyber security
- Traffic flow
- Human-systems integration
- Crowd dynamics
- Human behavior

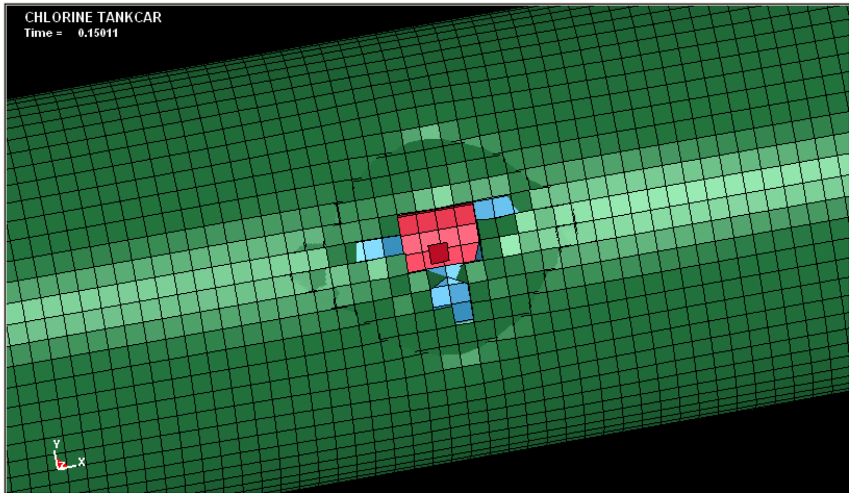
Example M&S tools for many of these areas are cited in the next section. Mention of a specific M&S tool does not imply endorsement.

Structural Mechanics/Dynamics Simulations

- Typical Applications:
  – Finite element analysis
  – Dynamic load analysis
- Examples:
  – NASTRAN (originally from “NASA Structural Analysis” in the late 1960s)
  – LS-DYNA® (Livermore Software Technology Corp.)



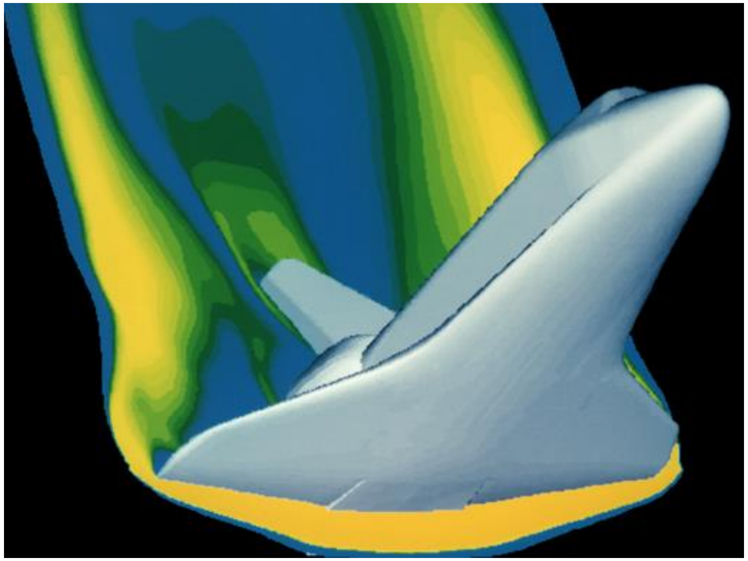
MSC Nastran result (source: Wikipedia)



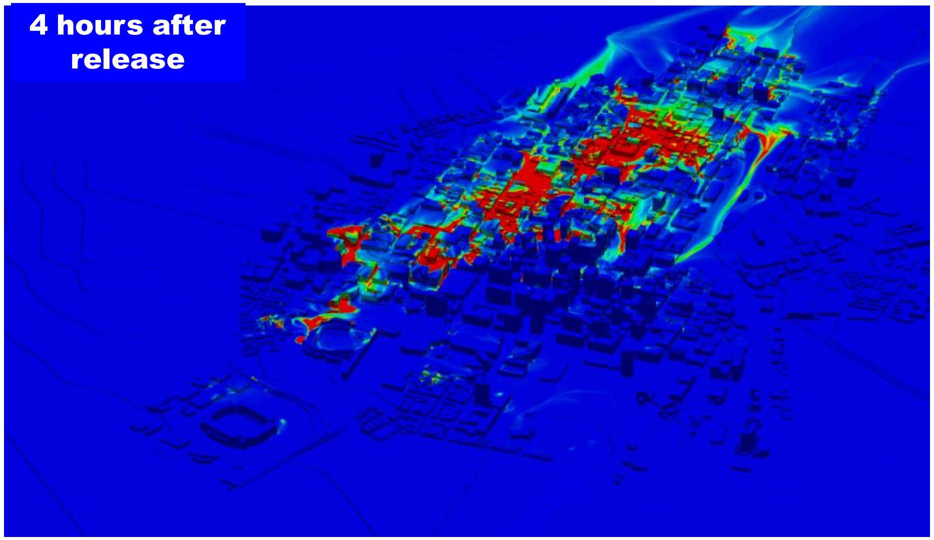
LS-DYNA result of explosive rupture of railcar (source: Florida A&M University)

Fluid Dynamics Simulations

- Typical Applications:
  - Air flow around solid shapes
  - Hydrodynamic analysis
- Examples:
  - ANSYS (www.ansys.com)
  - HYB-3D (University of Alabama at Birmingham)



Flow around the Space Shuttle (source: NASA)



Chlorine spill dispersion in an urban area (source: UAB)

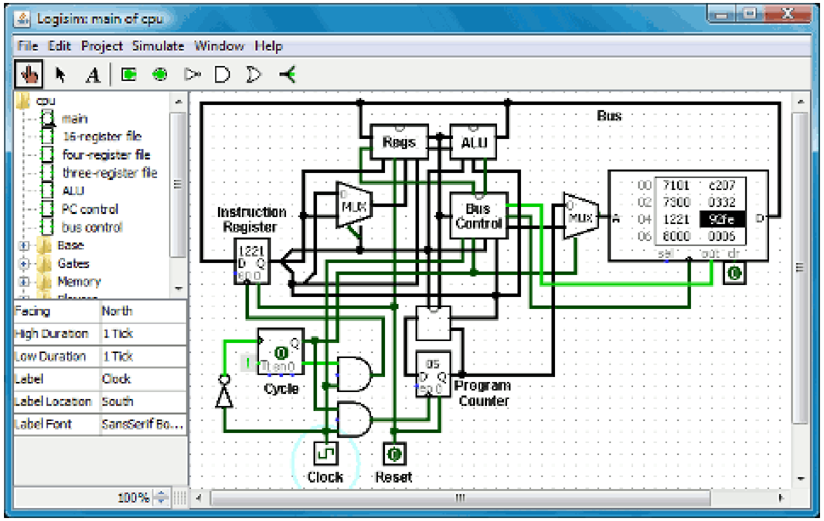
Materials Engineering Models

- Typical Application:
  - Predicting fatigue crack growth in structures
- Example:
  - AFGROW (Air Force Growth)

Example of crankshaft fatigue (source: Wikipedia)

Printed Circuit Design Simulations

- Typical Applications:
  - Simulation of electrical circuit board behavior during design
- Examples:
  - SPICE (Simulation Program with Integrated Circuit Emphasis)
    - 1973 Cal Berkeley, open source, spawned commercial variants
  - Logisim (digital circuits only, open source, student audience)



Screen shot of Logisim 2.3.4, released April 1, 2010 (source: Hendrix College web site)

Electrical Power System Design Simulations

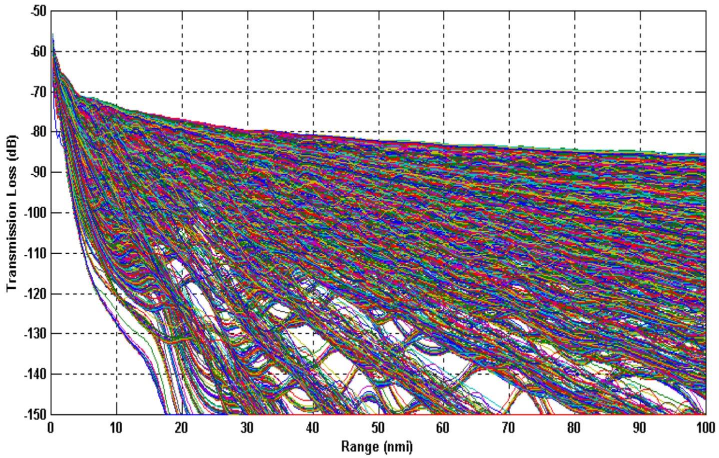
- Typical Applications:
  - Simulation of power systems for buildings and communities
  - Simulation of a regional or national electric power grid
- Examples:
  - eMEGAsim – OPAL-RT Technologies
  - RTDS® (Real Time Digital Simulator) – RTDS Technologies

Computer Network Engineering Simulations

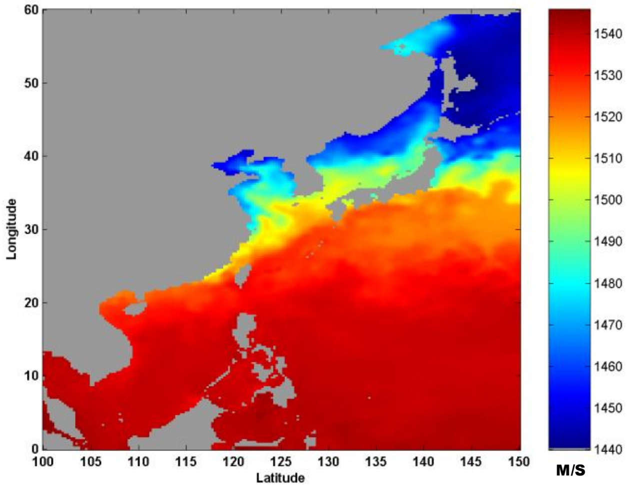
- Typical Applications:
  - Design and performance evaluation of computer networks
  - Simulation of natural and man-made network disruptions
- Examples:
  - OPNET Modeler
  - Joint Communication Simulation System (JCSS) [formerly NETWARS]

Acoustic Propagation Models

- Typical Applications:
  - Determination of detection ranges for underwater sound sources
  - Determination of sound speed based on environmental features
- Examples:
  - Automated Signal-Excess Prediction System (ASEPS) Transmission Loss (ASTRAL)
  - Modular Ocean Data Assimilation System (MODAS)



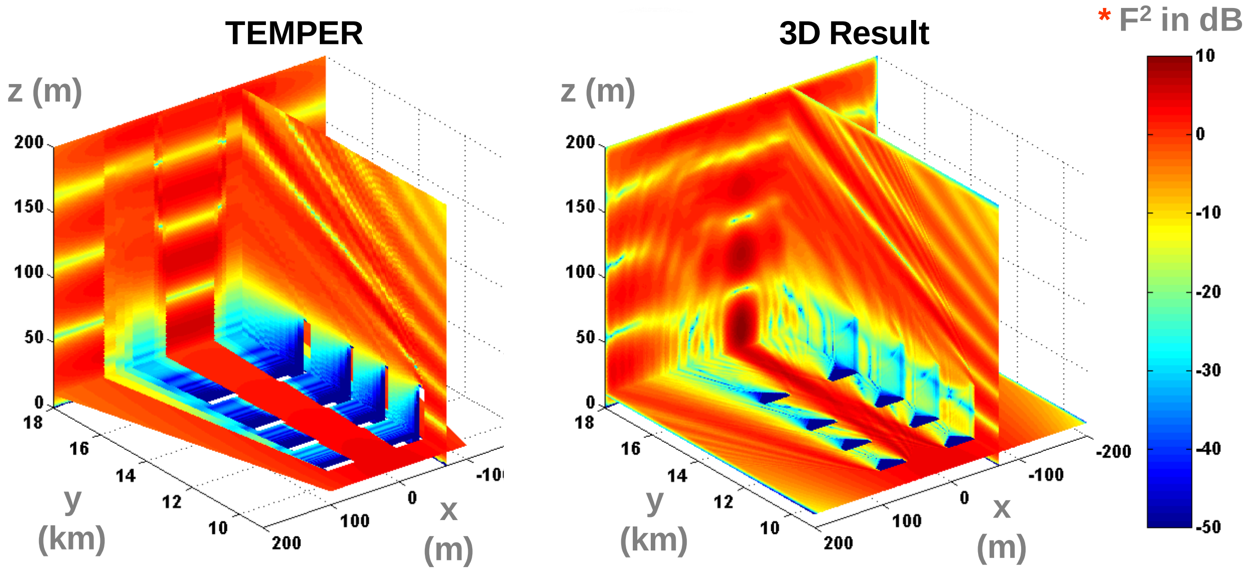
ASTRAL transmission loss curves (source: Biondo & Mandelberg – MIV project)



MODAS surface sound speed (source: Biondo, Mandelberg et al – JWARS-MIV project)

Electromagnetic Propagation Models

- Typical Application:
  - Determination of atmospheric detection ranges for electromagnetic sources
- Example:
  - Tropospheric Electromagnetic Parabolic Equation Routine (TEMPER)

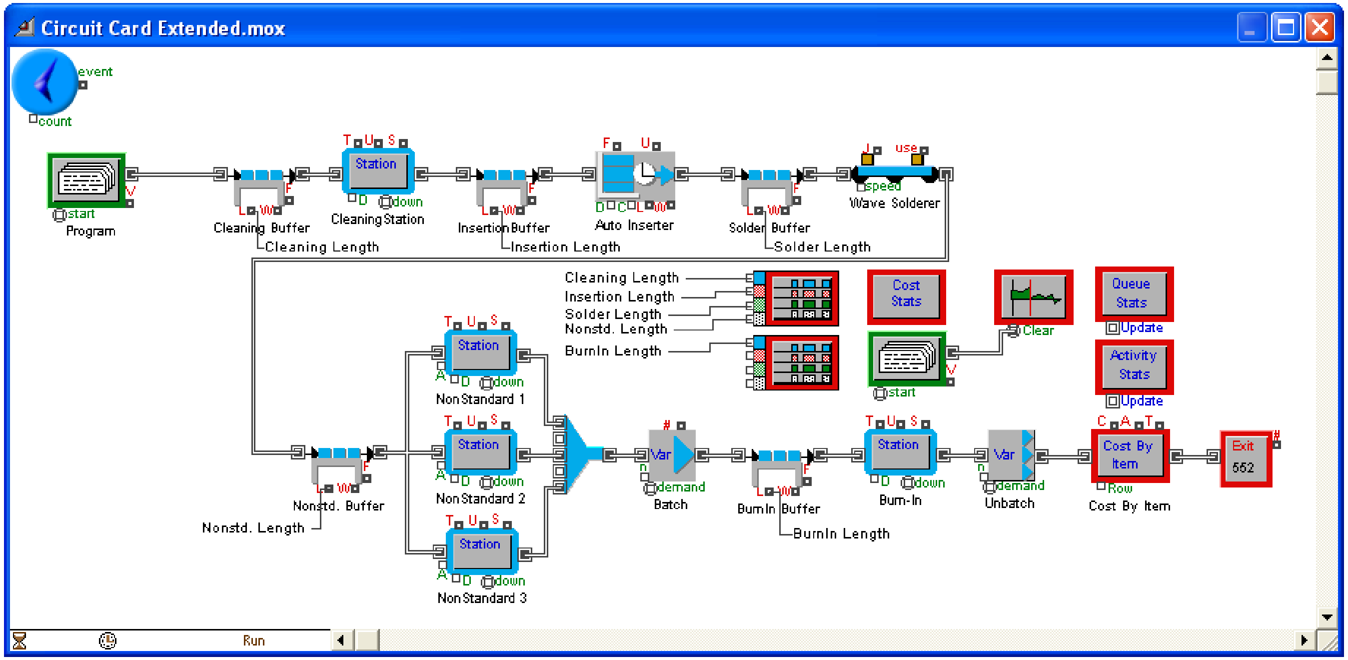


* **Propagation factor "F" ≡ | E / E_o| where E_o is free-space field**

Source: Awadallah, et al, Radar Propagation in 3D Environments, 2004

Manufacturing Process Models

- Typical Applications:
  - Determining and optimizing production rates
  - Determining bottlenecks in planned production lines
- Examples:
  - ExtendSim
  - Arena



Source: Strickland, Discrete Event Simulation Using Extend, 2009

Integrating Engineering-Level Simulations

- The process of integrating engineering-level simulations is similar to the process of integrating a system
  - Each simulation acts as a component of the integrated simulation (often referred to as a "federation" of simulations)
  - Data interchange agreements for simulations are like interface control documents for systems
- Engineering-level simulations can be integrated with one another
  - Through sequential passing of data from one simulation to the next
    - Possible if there are no significant "feedback" paths
    - Can be done through automation, or manually (a.k.a. "sneaker net")
  - Through run-time interoperability (e.g., using the High Level Architecture for simulation interoperability, IEEE 1516)
    - Requires pre-execution agreements as to which simulations "publish" and "subscribe to" data elements
    - Requires a run-time infrastructure to manage execution

Integrating Engineering-Level Simulations Through Sequential Data Passing

- Need to establish that a given simulation produces outputs that are compatible with inputs required by the next simulation in the sequence, either directly, or by some well-defined transformation
  - "Post-processing" and/or "pre-processing" steps may be required to ensure output-input compatibility
- "Syntactic" interoperability – refers to ensuring that the (post-processed) data outputs are the same data element and are in the same units of measure as the (pre-processed) data inputs
- "Semantic" (or "substantive") interoperability – refers to ensuring that the (post-processed) data outputs and (pre-processed) data inputs have the same meaning in both simulations
  - For example, if a simulation generating "speed" data assumes over-the-ground speed and the data-receiving simulation assumes through-the-air speed, there is no semantic interoperability
- Both syntactic and semantic interoperability are needed for two simulations to be "composable"

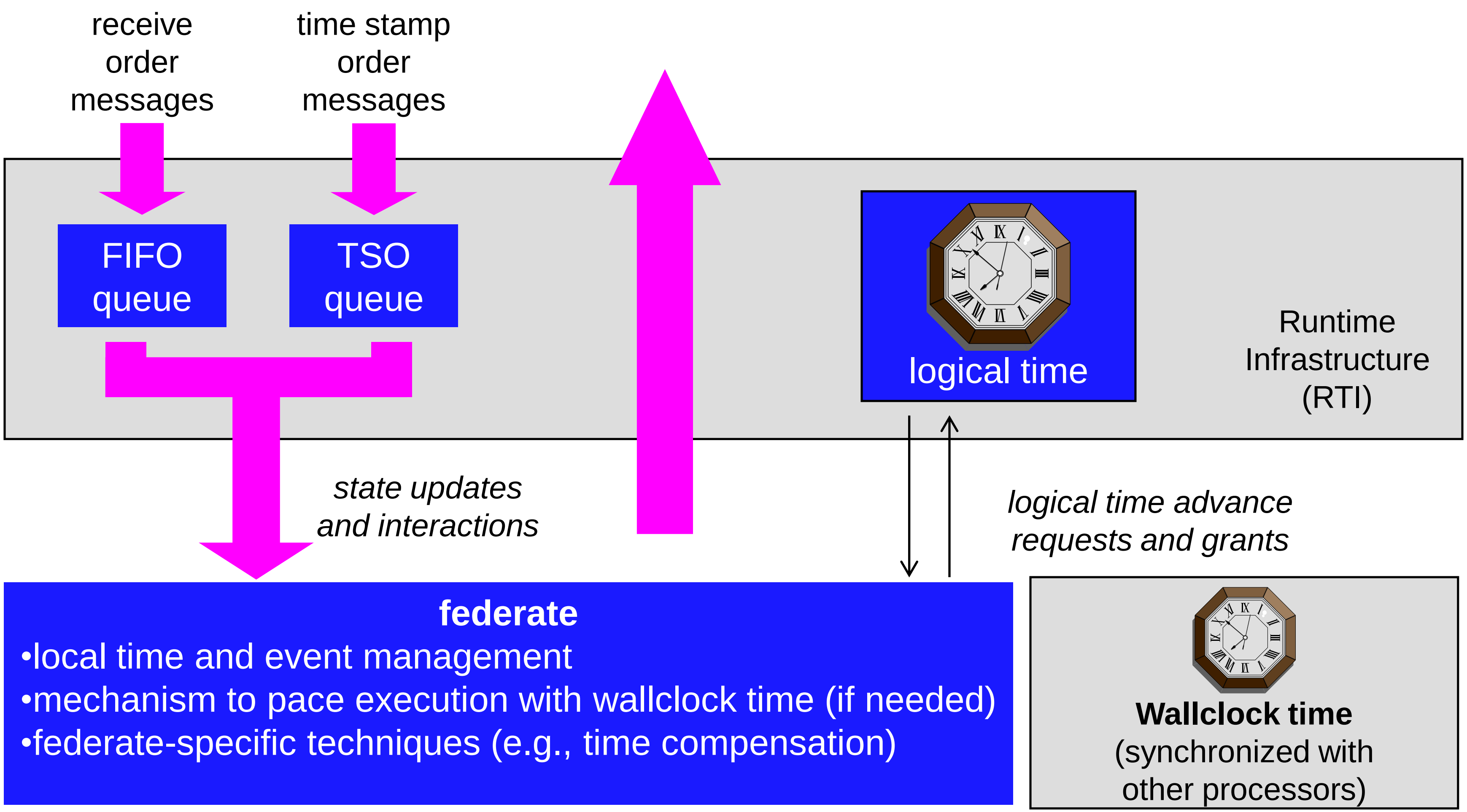
Integrating Engineering-Level Simulations Through Run-Time Interoperability

- Most engineering-level simulations require
  - Causality: The effects of an action are observed after the action occurs
  - Repeatability: The simulation gives the same result if executed twice
- Ensuring causality and repeatability requires a method for maintaining “event ordering” at run-time
  - This is a non-trivial problem when executing several simulations interactively across a network, in which packets may arrive in a different order from the order in which they were generated
- Other issues for simulations interacting at run-time
  - Maintaining a consistent environment (terrain, weather) over time
  - Deciding which simulation should have control of an entity at a given time
  - Managing the number of interactions required (e.g., having a maximum range for a sensor so not every sensor-target pair needs to be evaluated)
  - Detecting that another simulation has stopped executing

Time Management in Simulations Interoperating at Run-Time – Time Definitions

- Wallclock time - The actual time of day during a simulation execution (e.g., today from 4 pm to 6 pm)
- Physical time - The time in the physical system being modeled being modeled by the simulation (e.g., from midnight to 6 pm on December 7, 1941)
- Simulation time (logical time) - The simulation's representation of physical time (e.g., double-precision floating point number between 0 and 18, where a simulation time unit represents an hour of physical time)
- Federate time - The logical (simulation) time within a particular simulation federate at any instant during a distributed simulation execution

A Logical View of Time Management (from the High Level Architecture)



from Fujimoto 1998, “Time Management in the High Level Architecture,” Figure 2

Module Summary

- A broad range of engineering disciplines are involved in design and development, thus requiring a broad range of models and simulations, primarily at the engineering level.
- A systems engineer responsible for M&S needs to have a broad view of M&S tools that can be applied in a range of disciplines during this phase.
- The process of integrating engineering-level simulations is similar to the process of integrating a system
- Engineering-level simulations can be integrated with one another
  - Through sequential passing of data from one simulation to the next
  - Through run-time interoperability
- Both syntactic and semantic interoperability are needed for two simulations to be composable
- Most engineering-level simulations require causality and repeatability
- Event ordering and time management are important for engineering-level simulations with run-time interoperability requirements

Modeling and Simulation
in Integration and Test & Evaluation

Module Objective and Outline

Module Objective: To describe the use of modeling and simulation in the integration and test & evaluation phase of the systems engineering process; and to describe special issues particular to this phase.

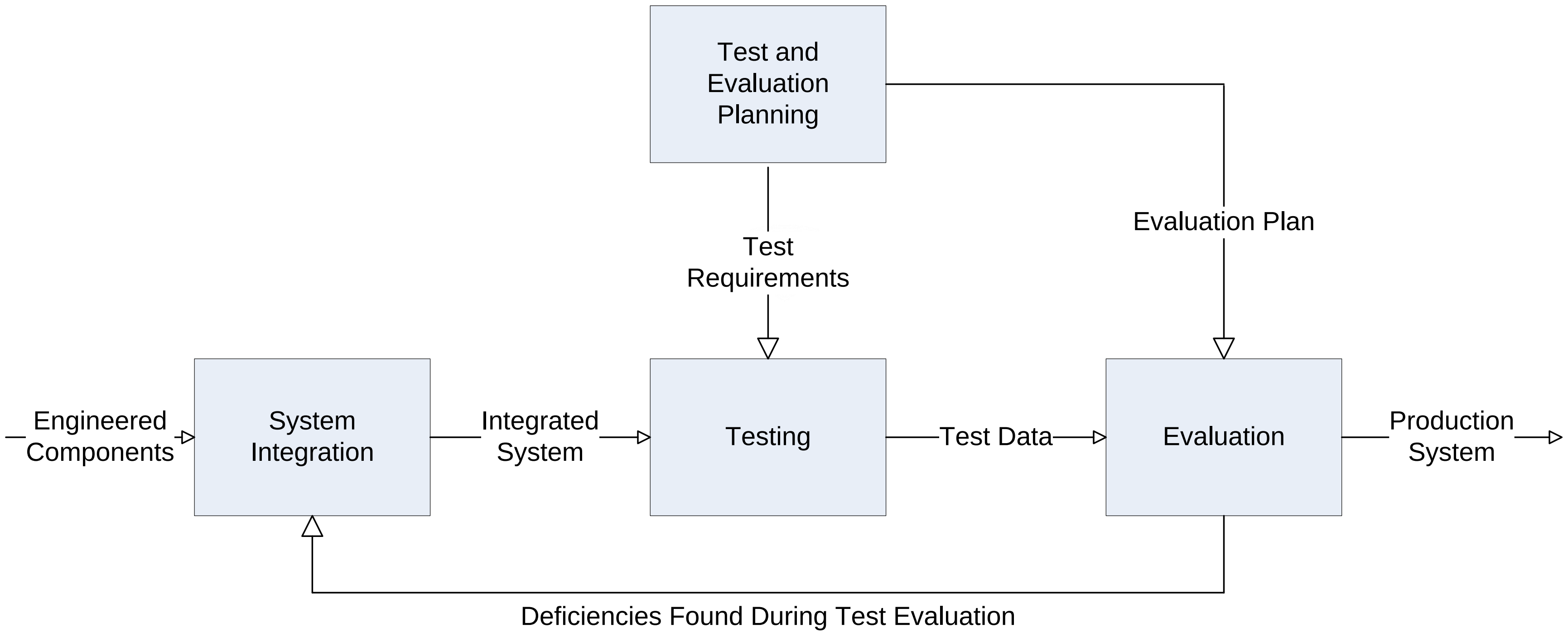
Module Outline

- Scope of Integration and Test & Evaluation (T&E)
- A Simplified Process Model for Integration and T&E
- Simulation Use During Integration
- Planning for Use of Models and Simulations During T&E
- Simulation Use During Testing
- Post-Test Evaluation Using Models and Simulations
- Summary

Scope of Integration and Test & Evaluation (T&E)

- The integration and T&E phase of systems engineering, as discussed in this course, corresponds to the Integration and Evaluation phase in the Kossiakoff and Sweet textbook
- Integration takes unit-tested components and subsystems and forms them into an integrated system
- Test and evaluation (T&E) of military systems is typically divided into
  - Developmental test and evaluation (DT&E) conducted under the auspices of the system's program manager
  - Operational test and evaluation (OT&E) conducted by an independent operational test agency (OTA)
- Integration and test activities are typically aided by live, virtual, and constructive simulations running at or near real time
- Evaluation activities sometimes involve models of the system and its components to aid in determining the source of unexpected test performance

A Simplified Process Model for Integration and T&E



Simulation in Integration – Use of Stimulators

- As one proceeds from unit testing to system integration, there is often a need for "stimulators" to represent a part of the system (or the external environment) that is not currently available for integration
- Examples of stimulators:
  - Generation of an infrared (IR) scene to be sensed by an IR seeker
  - Representation of a radar (or other sensor) output as it would be presented to its processing system
  - Representation of a potential human operator's input to a vehicle control system
- Gradually substitute real system components for simulated system components until full system is integrated

Simulation Issues of Particular Interest During Integration

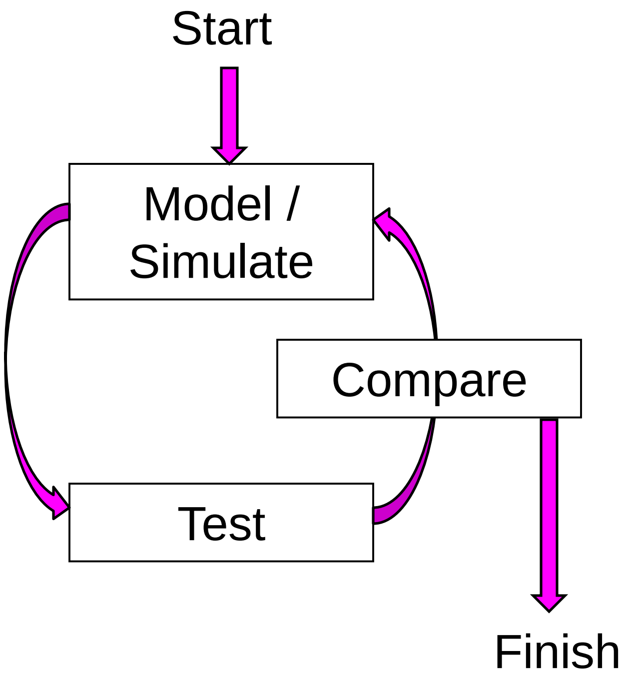
- Representativeness of integration environment as compared to the intended operational environment
  - Are characteristics of the simulated external environment sufficiently realistic, in terms of frequency, intensity, etc.?
- Real-time operation (often “hard-real-time”)
  - Can the software simulation of a hardware component operate quickly enough?
  - Can simulation/stimulation components adequately represent the frequency and periodicity of the real system components?
- Similarity of simulator/stimulator interfaces to those of the objective system component
  - Are the interfaces of the simulator/stimulator the same as those of the system component being represented? Or sufficiently similar so that differences can be accommodated without sacrificing realism?

Planning for Use of Models and Simulations During T&E

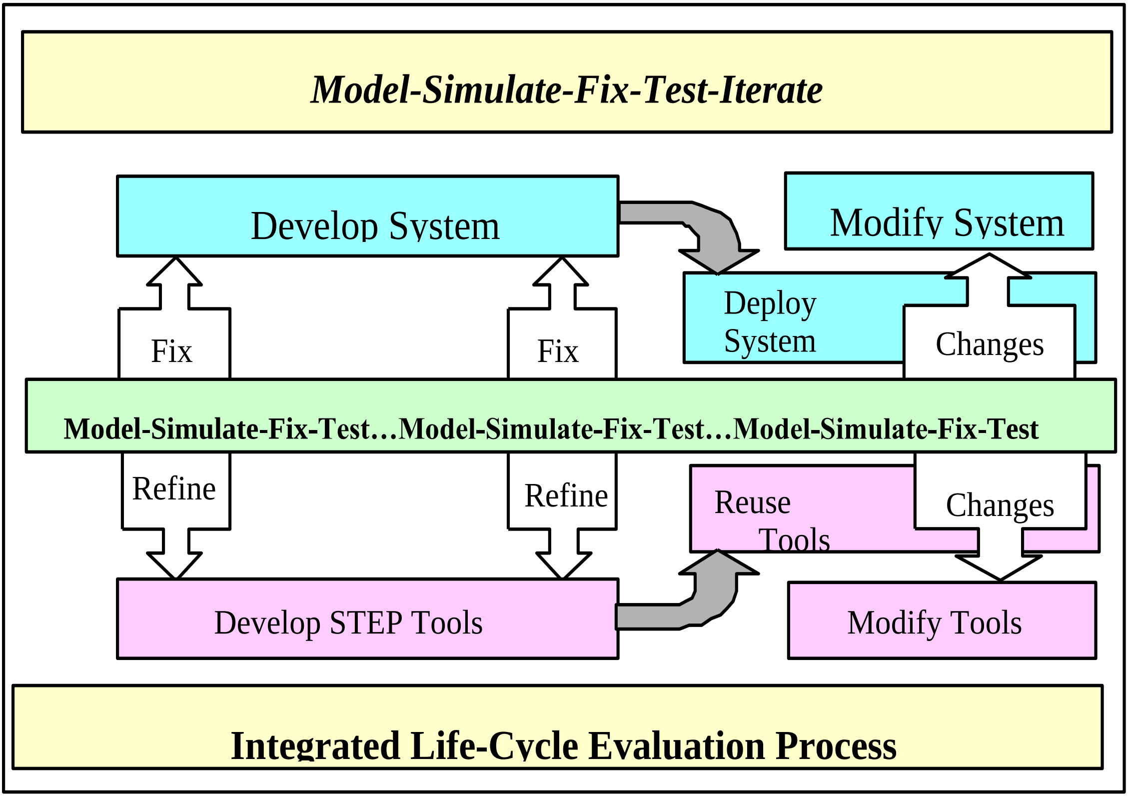
- Need to determine the appropriate integrated combination of models, simulations, and test events to obtain the most credible data with which to conduct a comprehensive evaluation of system performance
  - Are there situations where safety precludes testing?
  - Are there physical constraints (e.g., size of test range)?
  - Are there fiscal constraints (e.g., for system of systems testing)?
- Need to identify areas where actual testing either can be augmented by M&S or used to validate the models and simulations
- Need to summarize the model, simulation, and data verification, validation, and accreditation (VV&A) to be conducted
- Need to document how the integrated use of accredited models and simulations with operational testing will increase the knowledge and understanding of the capabilities and the limitations of the system as it will be employed
- Need to include the resources required to perform VV&A of the models and simulations; to obtain and maintain the models and simulations; and the resources required to archive data

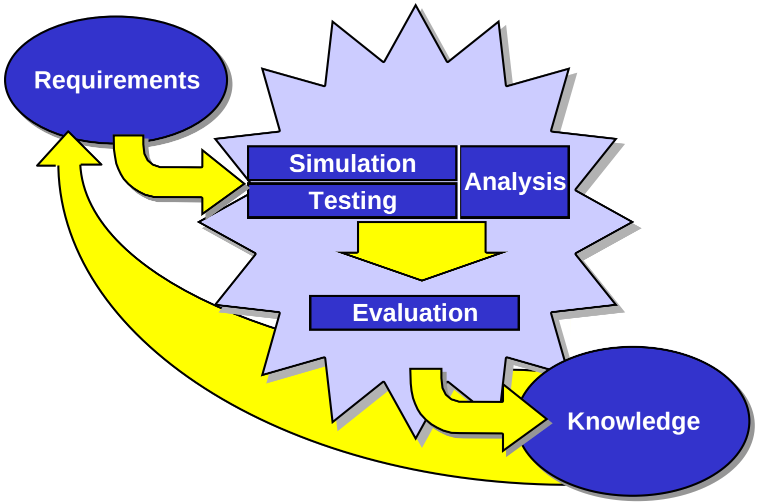
The Model-Test-Model (MTM) Paradigm

- The Model-Test-Model (MTM) paradigm refers to the iterative use of models & simulations and testing to refine the modeled representation of a system
- Start with a best estimate of the system's performance as represented in a model or simulation
- Conduct testing on the (prototype) system to collect data on how the system performs in reality
- Use the data collected to refine the modeled representation of the system's performance
- Repeat as necessary until the modeled representation of the system is deemed adequate



The Simulation Test and Evaluation Process (STEP) – a 1990s DoD Attempt at Integrating M&S and T&E





Source: Simulation, Test, and Evaluation Process (STEP) Guidelines, Director, Operational Test and Evaluation, and Director, Test, Systems Engineering and Evaluation, 4 Dec 1997.

Hardware- and Software-in-the-Loop Simulations For Testing

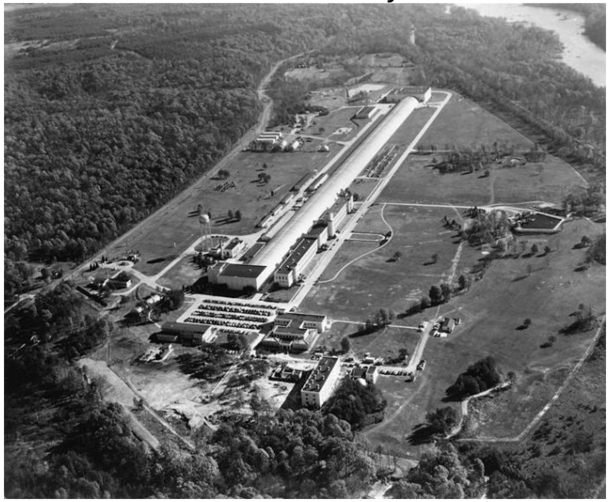
- Hardware-in-the-loop (HWIL) simulations are a good example of simulations that are generally not (or need not be) computer-based
  - Examples:
    - Wind tunnels for missiles and aircraft
    - Anechoic chambers for radar seekers
    - Scene generators for focal plane arrays
    - Tow tanks for maritime vehicles
    - Pressure chambers for submersible vessels/housings
    - Crash-test facilities for automobiles
    - Shake tables for mechanical structures
    - Vacuum chambers for spacecraft
  - Require calibrated instrumentation to collect data on the system under test
- Software-in-the-loop (SWIL) simulations embed actual system software in a synthetic environment representing the system's intended use

Examples of HWIL Facilities

NASA wind tunnel with aircraft model

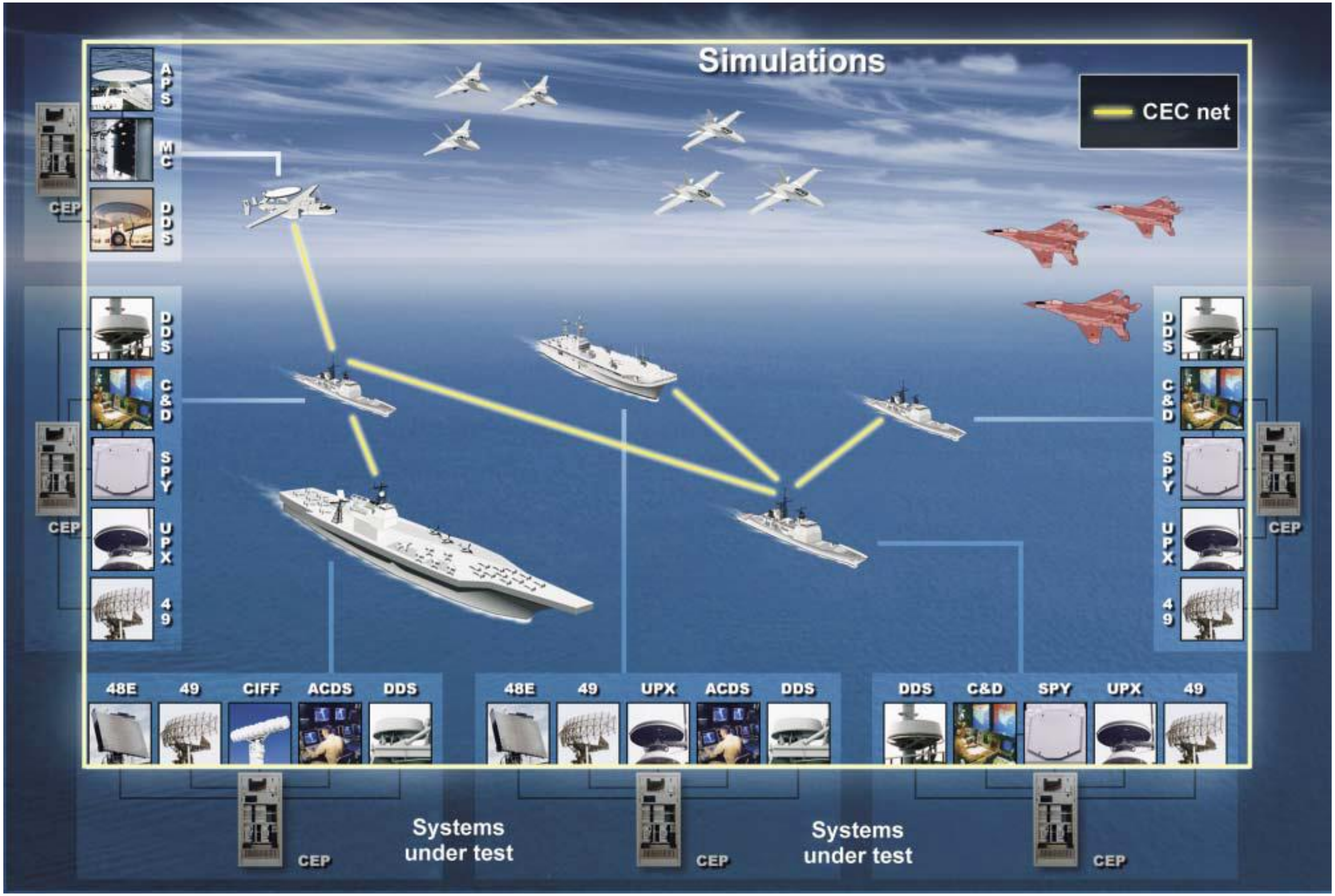
Benefield Anechoic Facility at Edwards Air Force Base

NHTSA crash test



David Taylor Model Basin, Carderock

SWIL Example – JHU/APL Cooperative Engagement Processor (CEP) Wrap-Around Simulation Program (WASP)



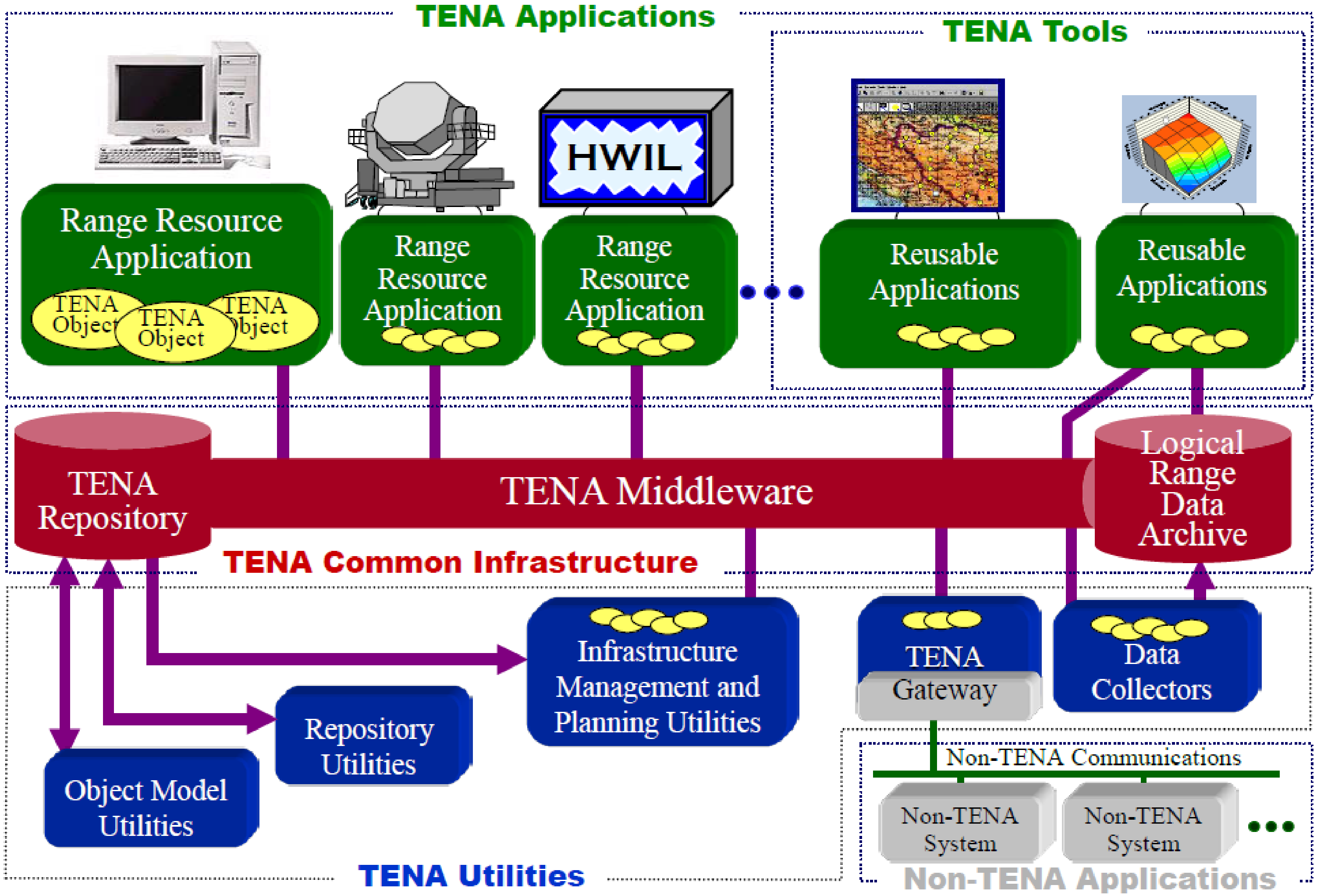
Pre-Test Predictions Using Models and Simulations

- In modern-day system acquisition, having a (perceived) failure during a highly visible system test can de-rail the system development process
- By modeling the system's performance in the test environment prior to the actual test, one can
  - Vary environmental parameters to determine if there are any situations in which the test should be delayed because of excessive risk (e.g., extreme wind shear conditions, extreme hot or cold temperatures)
  - Establish an "objective" benchmark with which to compare the actual test results
    - Aids in determination as to whether the test was "successful"
  - Determine boundaries of realistically expected performance, for evaluating/ensuring safety during the test
    - For example, "three-sigma" ballistic missile trajectory envelopes for range-safety decisions on whether to destroy the missile

Simulation Use in Test Range Activities

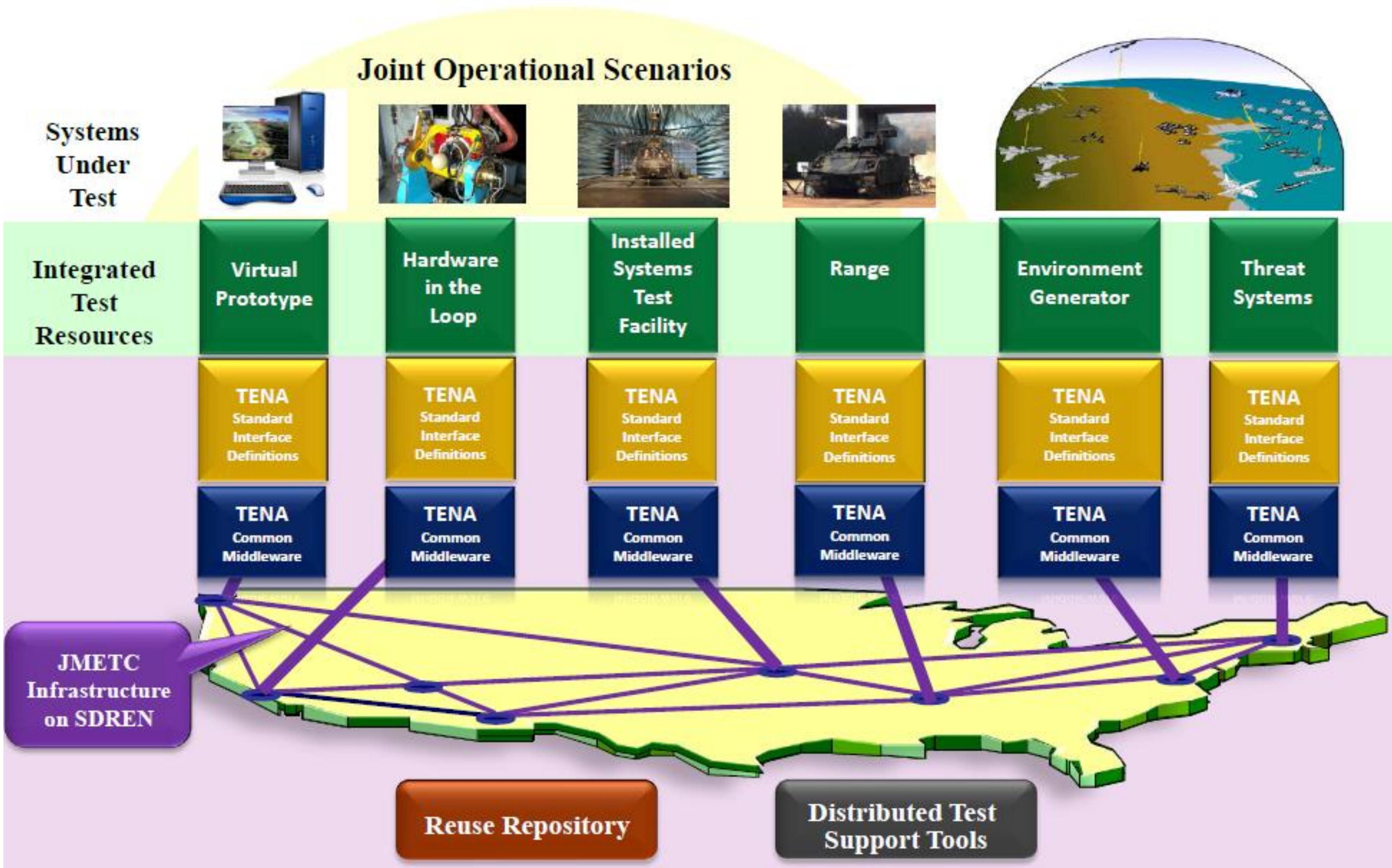
- Simulate assets (targets, friendly systems/platforms) not available in the range environment using constructive simulations
  - For large scale “system-of-systems” tests requiring demonstration of inter-system interoperability
- Supplement natural environment on the test range with simulated natural environment features not present on the test range
- “Geo-relocate” live test assets from other test ranges

TENA Architecture Overview



Source: "Test and Training Enabling Architecture (TENA) Overview," Oct. 2015 (available at https://www.tena-sda.org)

Joint Mission Environment Test Capability (JMETC) Distributed Test Architecture



Source: "Test and Training Enabling Architecture (TENA) Overview," Oct. 2015 (available at https://www.tena-sda.org)

Simulation Issues of Particular Interest During Testing

- Latency of transmissions across the network of constructive, virtual, and live assets
  - Need to maintain representative “real-time” interactions
- Bandwidth of networks
  - For example, environmental data often needs to be “pre-loaded” because of bandwidth constraints
- Time synchronization among geographically distributed systems
  - GPS time source often used
- Consistency of environmental representations across live, virtual, and constructive simulation assets
- Potential safety issues introduced by adding constructive or virtual targets to a live display
  - For example, introducing simulated threat aircraft in a heads-up cockpit display could result in evasive maneuvers into a real mountain

Post-Test Evaluation Using Models and Simulations (1 of 2)

- Single-test results
  - Comparison of test results to pre-test model/simulation predictions
  - If results differ from predictions:
    - Are test results within a statistically-expected range?
    - Are there differences in the day-of-test environment from the predicted environment?
      - If so, can do a “post-test prediction” based on the day-of-test environment
    - Does test data indicate an obvious anomaly in performance?
  - If differences appear to be “real”:
    - Is there an algorithmic error in the model/simulation?
    - Is there an un-modeled effect that could account for the difference?
    - Is it appropriate to “calibrate” the model/simulation based on a single test?

Post-Test Evaluation Using Models and Simulations (2 of 2)

- Multiple-test results
  - Comparison of multiple test results to pre-test (or post-test) model/simulation predictions
  - Unfortunately, except for “high-value systems” (e.g., Navy Trident missile system), it is seldom possible to conduct enough full-system tests to get statistically significant results
  - Is there a pattern (bias) of the test results when compared to the model/simulation predictions? If so,
    - Is there an algorithmic error in the model/simulation?
      - Can use of statistical modeling techniques (e.g., Kalman filter) help to reveal the source of the error?
    - Is there an unmodeled effect that could account for the difference?
    - Is it appropriate to “calibrate” the model/simulation based on this number of tests?

Example of Multi-Test Evaluation JHU/APL Trident II Accuracy Evaluation

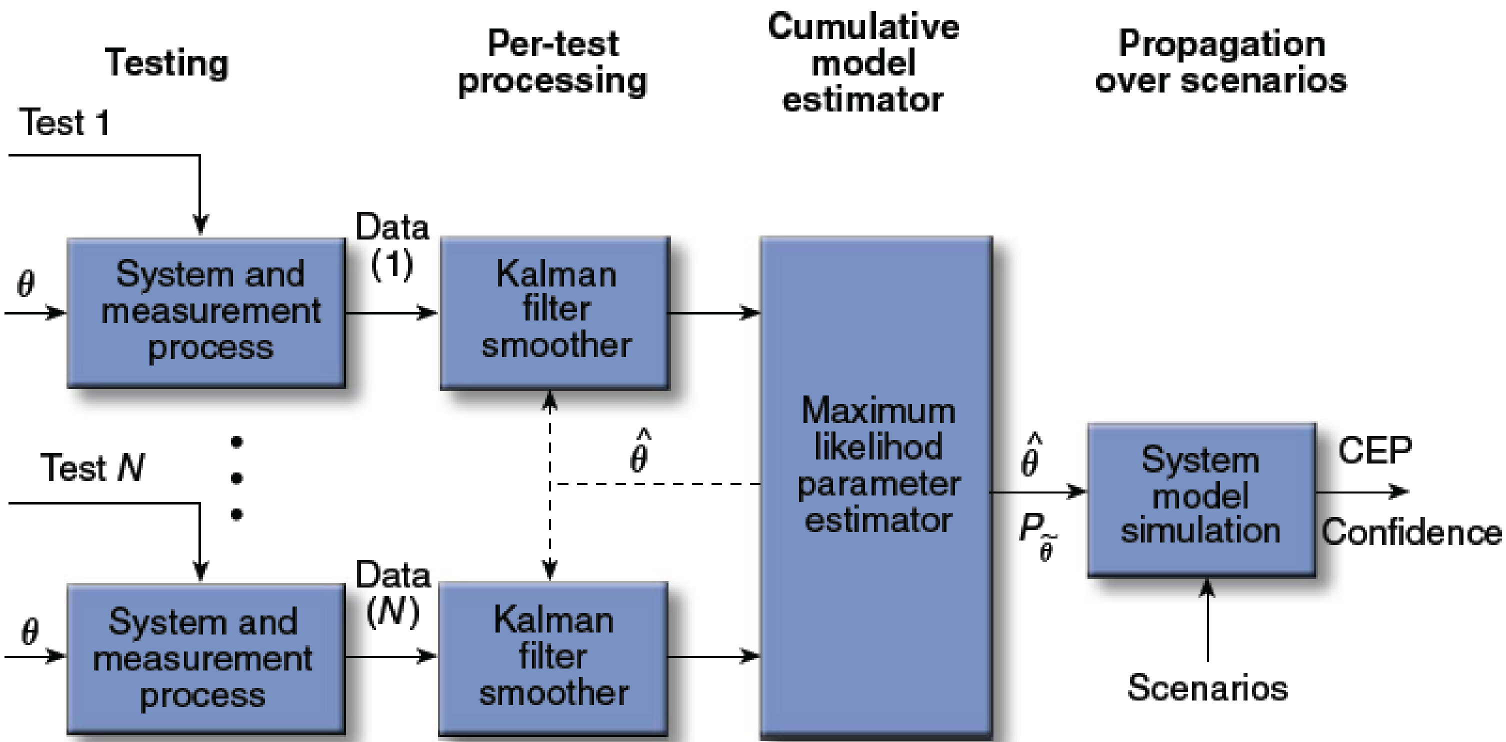


Figure 5. Model estimation for Trident II resulting in the credible performance prediction of a critical system to the government and military system. (θ = true model parameter vector, $\hat{\theta}$ = estimate of θ, $P_{\tilde{\theta}}$ = covariance of estimation error in θ.)

Source: Levy, L.J., “”The Systems Analysis, Test, and Evaluation of Strategic Systems,” APL Tech. Digest, Vol. 26, No. 4 (2005), pp. 438-442.

Module Summary

- In system testing, there is often a need for “stimulators” to represent a part of the system (or the external environment) that is not currently available for testing
- Use of models and simulations during T&E must be planned well in advance, in conjunction with the overall T&E plan
- Models and simulations are instrumental in pre-test predictions of system performance
- Simulations are essential to represent assets (threat and friendly) not available for system testing
- Models of the system under test and its components are useful in determining the specific source of differences between pre-test predictions and system test performance

Coolahan Associates, LLC ™

JOHNS HOPKINS
WHITING SCHOOL of ENGINEERING

Modeling and Simulation in Production and Sustainment

Module Objective and Outline

Module Objective: To describe the use of modeling and simulation in the production and sustainment phase of the systems engineering process; and to describe special issues particular to this phase.

Module Outline

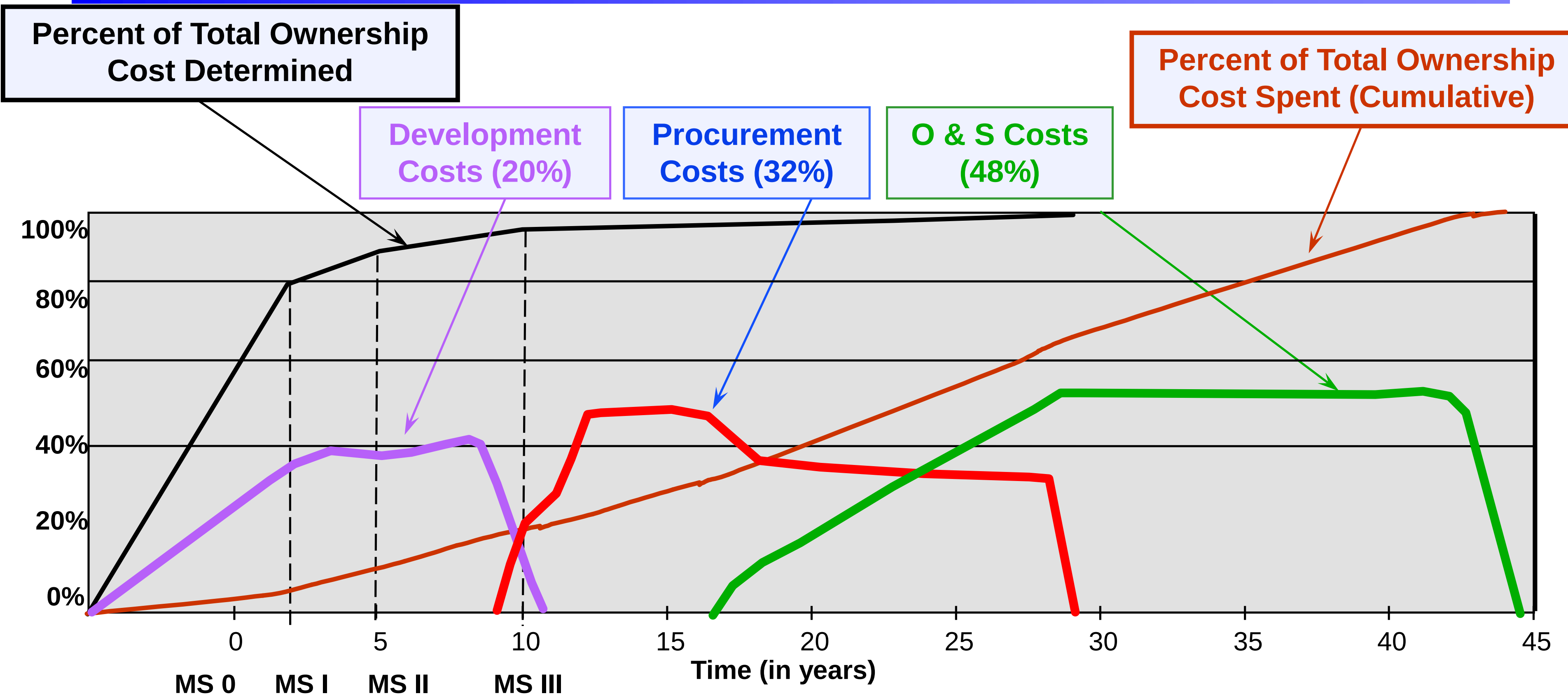
- Scope of Production and Sustainment
- A Simplified Process Model for Production and Sustainment
- Planning for Use of Models and Simulations During Production
- Model and Simulation Use During Production
- Model and Simulation Use During Sustainment
  - Systems Operation Simulations
  - Reliability Modeling
  - Logistics Simulations
  - Ownership Cost Modeling
- Summary

Scope of Production and Sustainment

- The Production and Sustainment phase of systems engineering, as discussed in this course, corresponds to the Post-Development Stage, consisting of the Production and Operations & Support phases, in *Systems Engineering: Principles and Practice* [1].
- Production takes the production design that results after Test & Evaluation, and "realizes" one or more instances of the system
  - Relatively straightforward for software-only systems
  - Can be quite complex for hardware systems
- Sustainment, which includes Operations and Support, is typically the lengthiest phase for a system, lasting as long as 60 years for large-scale military systems (e.g., aircraft carriers and the B-52 bomber)
  - Can incur up to 50% of the Total Ownership Cost (TOC) of a system
  - Planning for Sustainment (and Disposal) using models and simulations needs to occur early in the systems engineering process

Source: (1) Kossiakoff, A., Sweet, W. N., Seymour, S. J., and Biemer, S. N., *Systems Engineering: Principles and Practice, Second Edition*, John Wiley & Sons, Inc., Hoboken, N. J. (2011).

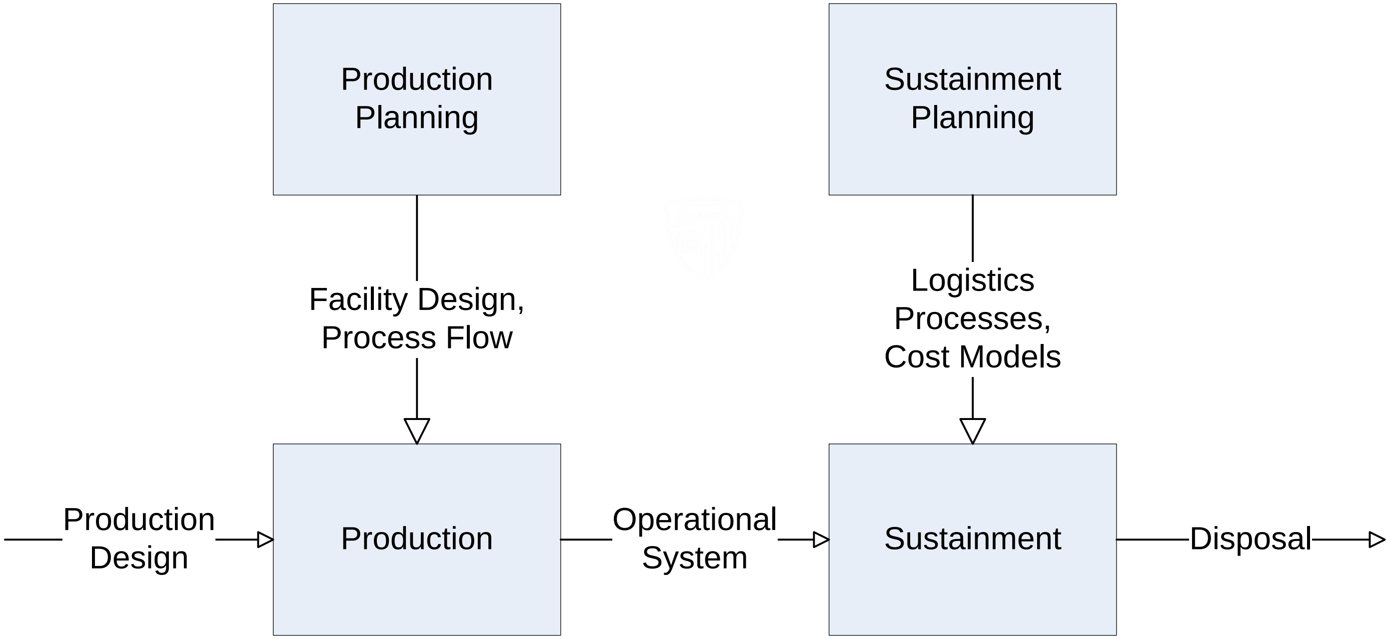
Military System Total Ownership Cost by Phase, and When Determined



Efficient Exploration of the Design Space Early in the Program Is Key to Reducing Total Ownership Cost

Source: *The Simulation Based Acquisition Vision: A Brief Tutorial*, Nicholas E. Karangelen, March 1998

A Simplified Process Model for Production and Sustainment



Planning for Production Using Models and Simulations

- Just as one needs to plan early for Test and Evaluation, one also needs to plan early for Production, particularly for hardware systems
  - What rate of production is required?
  - How large does a facility (do facilities) need to be?
  - What is a good production process?
- Ensuring that computer-aided design (CAD) models of the system produced during Design and Development can flow seamlessly into computer-aided manufacturing (CAM) equipment
- Modeling the design of production facilities (using CAD)
- Simulating the flow of the system assembly process (using process models, such as Arena)

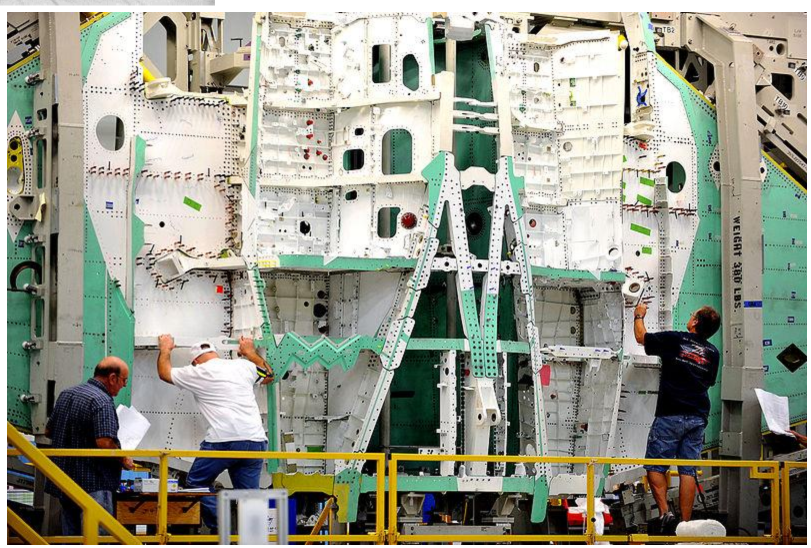
Model and Simulation Use During Production

- CAD models of the system produced during Design and Development are ingested by CAM equipment to automate component manufacturing
- Models of production manufacturing facilities created during Design and Development are refined, based on the production design of the system
- Simulations of the flow of the manufacturing process are executed, and the process iterated
  - To optimize the assembly line itself
  - To optimize the timing of the flow of component parts into the system assembly facility

Examples of Production Facilities

USAF TB-32 production line

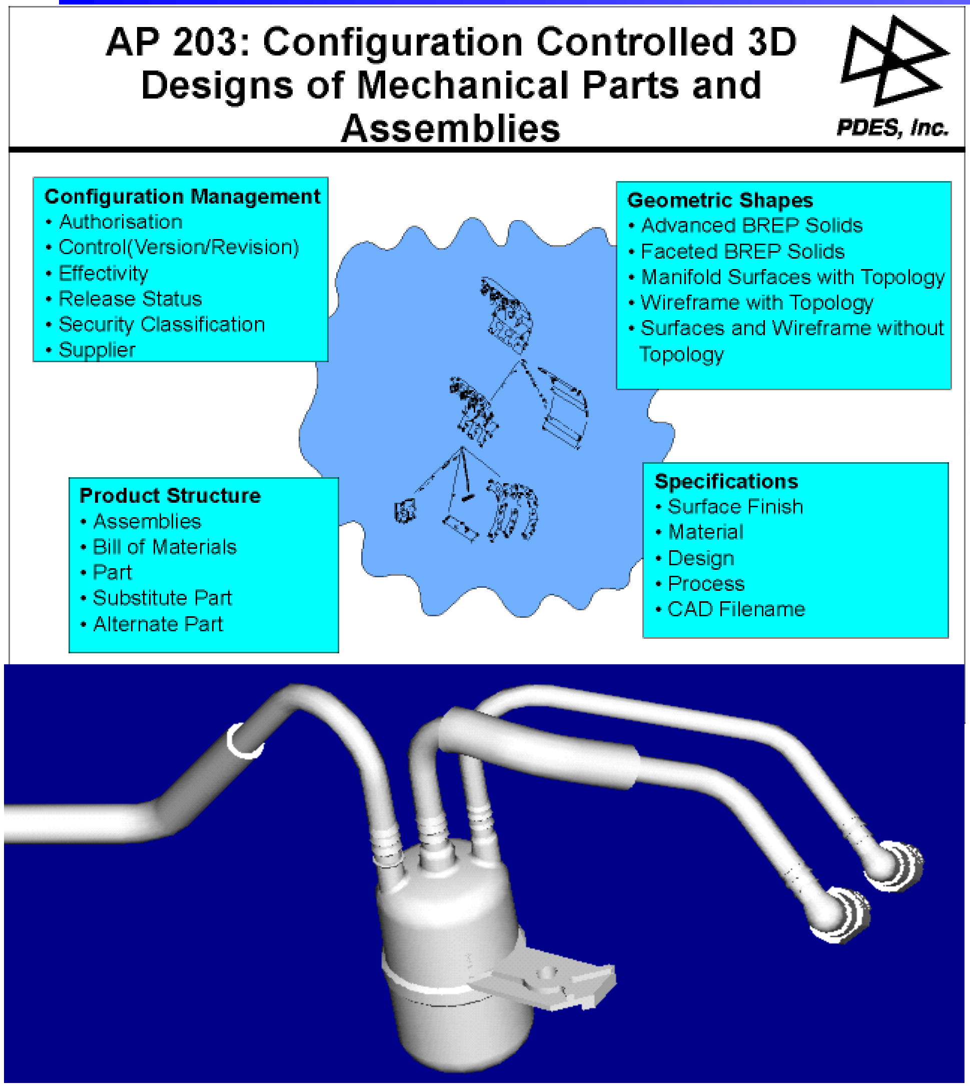
P-51D assembly line



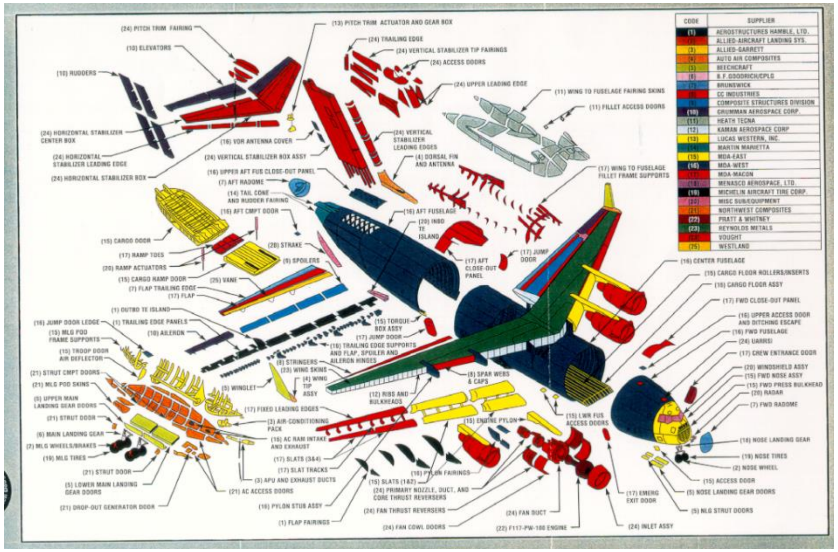
F-35 (Joint Strike Fighter) production facility

Source for photos: Wikimedia Commons. All of these photos are in the public domain.

M&S Standards in Production – Standard for the Exchange of Product Model Data (STEP)



- Boeing Commercial Aircraft
- Boeing CSTAR
- Delphi Automotive Systems
- Lockheed Martin
- NASA



Source: *Manufacturing Interoperability & the Manufacturing Systems Integration Division*, Steven Ray, Ph.D., National Institute of Standards and Technology, May 11, 2001

M&S Standards in Production – Core Manufacturing Simulation Data (CMSD) Standard

- Approved as a Simulation Interoperability Standards Organization (SISO) standard, spring 2010
- Utilizes Unified Modeling Language (UML) class and package diagrams
- CMSD information categories:
  - Calendar information
  - Resource information
  - Skill information
  - Setup information
  - Part information
  - Bill-of-materials information
  - Inventory information
  - Process plan information
  - Maintenance plan information
  - Order and Job information
  - Schedule information
  - Reference information
  - Probability distribution information

Model and Simulation Use During Sustainment

- Operations of the system are simulated under controlled conditions to reproduce system failures experienced in the operational environment, and to investigate potential solutions
- Reliability, Availability, and Maintainability of the system are modeled and re-modeled periodically, using data from systems in the operational environment
- Logistics for the repair and supply/re-supply of spare parts for the system are simulated
- Ownership costs are modeled on a continuing basis

Systems Operation Simulations

- Simulators replicating, as closely as possible, the system or major subsystems thereof, are often operated and maintained for high-value and high-volume systems
- Examples
  - Simulators for systems operating in a remote environment (e.g., system work-arounds for Apollo 13, unmanned interplanetary spacecraft)
  - Subsystem simulators to investigate infrequent operational problems (e.g., reported anomalous auto acceleration events)
  - Simulations of system component failures for accident forensics (e.g., space shuttle wing penetration by foam during launch)

Reliability, Availability, and Maintainability (RAM)

- Reliability – the probability that a system will perform its function correctly for a specified period of time under specified conditions
  - Typical metric: Mean Time Between Failure (MTBF)
- Maintainability – a measure of the ease of accomplishing the functions required to maintain a system in a fully operable condition
  - Typical metric: Mean Time To Repair (MTTR)
- Availability – the probability that a system will perform its function correctly when called upon
  - Typical metric: Probability of availability (P_A)
  - $P_A \approx 1 -$ MTTR / MTBF (for short repair times and low failure rates)
  - Note: Operational availability (A_o) is often used as a data element in military campaign simulations

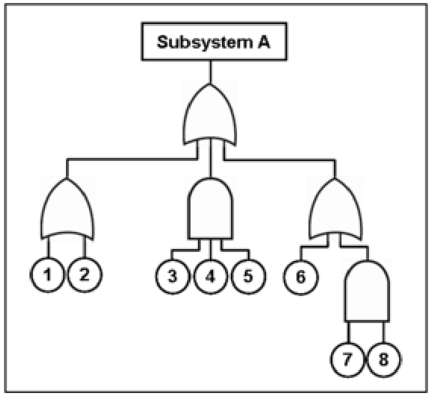
Source of definitions: *Systems Engineering: Principles and Practice*, Second Edition, Chapter 12

Reliability Modeling

- The reliability of a system can be modeled as a mathematical function of the reliability of its components
  - For a system of 10 critical independent non-redundant components,

    $P_R = P_{r1} \times P_{r2} \times \ldots \times P_{r10}$
  - For a system with two independent redundant components with failure probabilities P_{f1} and P_{f2},

    $P_R = 1 - P_{f1} \times P_{f2}$
- For a major system with many subsystems and components, the reliability model can become quite complicated, and is very dependent on accurate estimates of component reliabilities
- Example: Idaho National Laboratory (INL) SAPHIRE (*Systems Analysis Programs for Hands-on Integrated Reliability Evaluations*)
  - Implements Probabilistic Risk Assessment (PRA)
  - Used by NRC and NASA



Fault tree diagram

Repair and Spare Parts Logistics Simulations

- Similar to supply chain simulation during production of a system
- Essentially a process simulation tailored to the repair and supply/re-supply of spare parts for system support
- Various process modeling tools can be used
  - Arena
  - ExtendSim
  - AnyLogic
- Example logistics-specific models and simulations
  - Supply-Chain Operations Reference (SCOR) model
  - U.S. Air Force Logistics Simulation (LOGSIM)

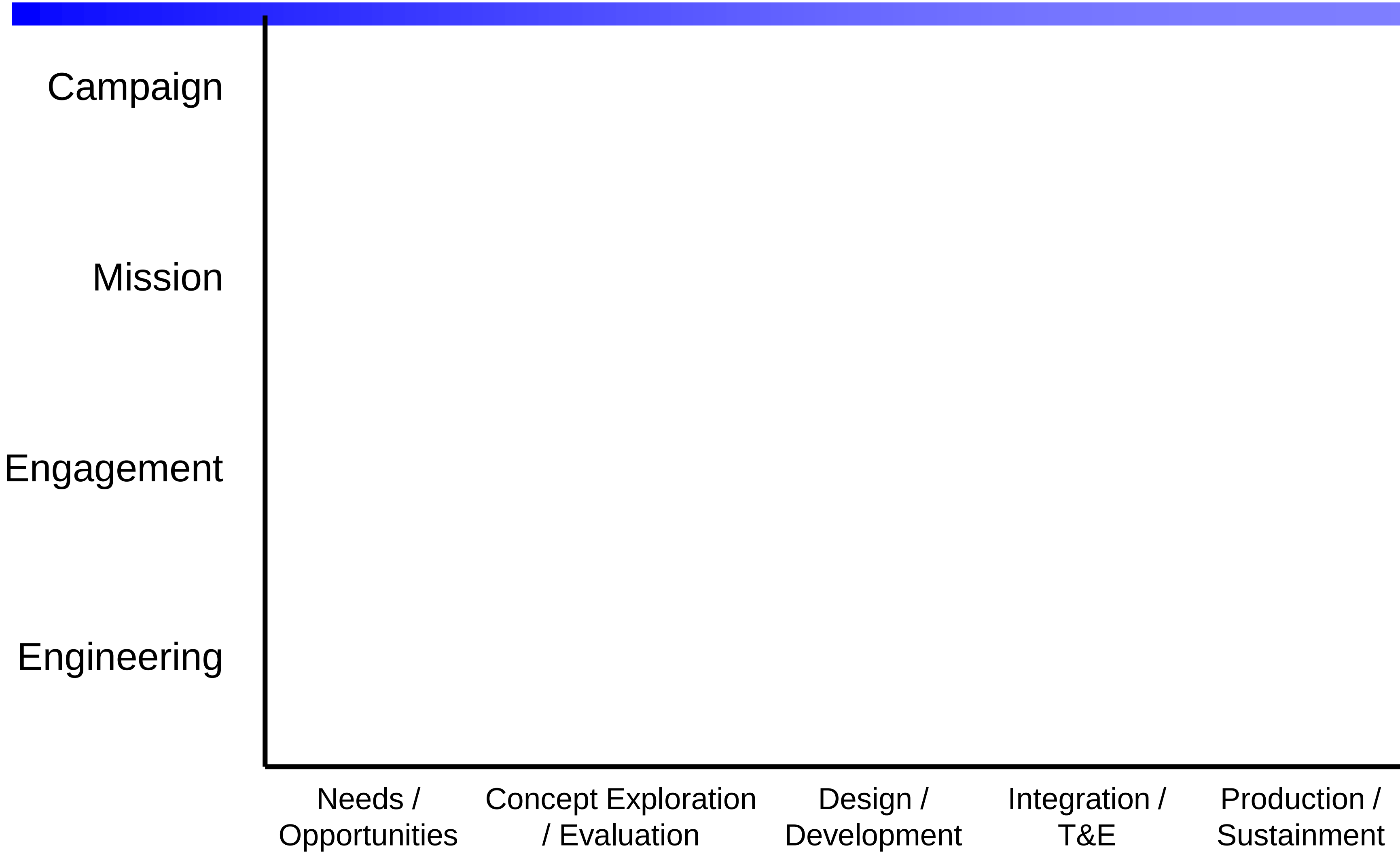
Ownership Cost Modeling

- Need to include all costs associated with continued ownership of a system
  - Personnel (operations and maintenance)
  - Fuel / power
  - Repairs and spare parts
  - …
- A variety of ownership cost models exist
  - ACEIT (Automated Cost Estimating Integrated Tools)
  - SEER-H (hardware), SEER-SEM (software) [Galorath]
  - Automotive System Cost Modeling (ASCM) Tool [Oak Ridge]
  - Cost Analysis Strategy Assessment (CASA) [US Army LEC]
  - …

Module Summary

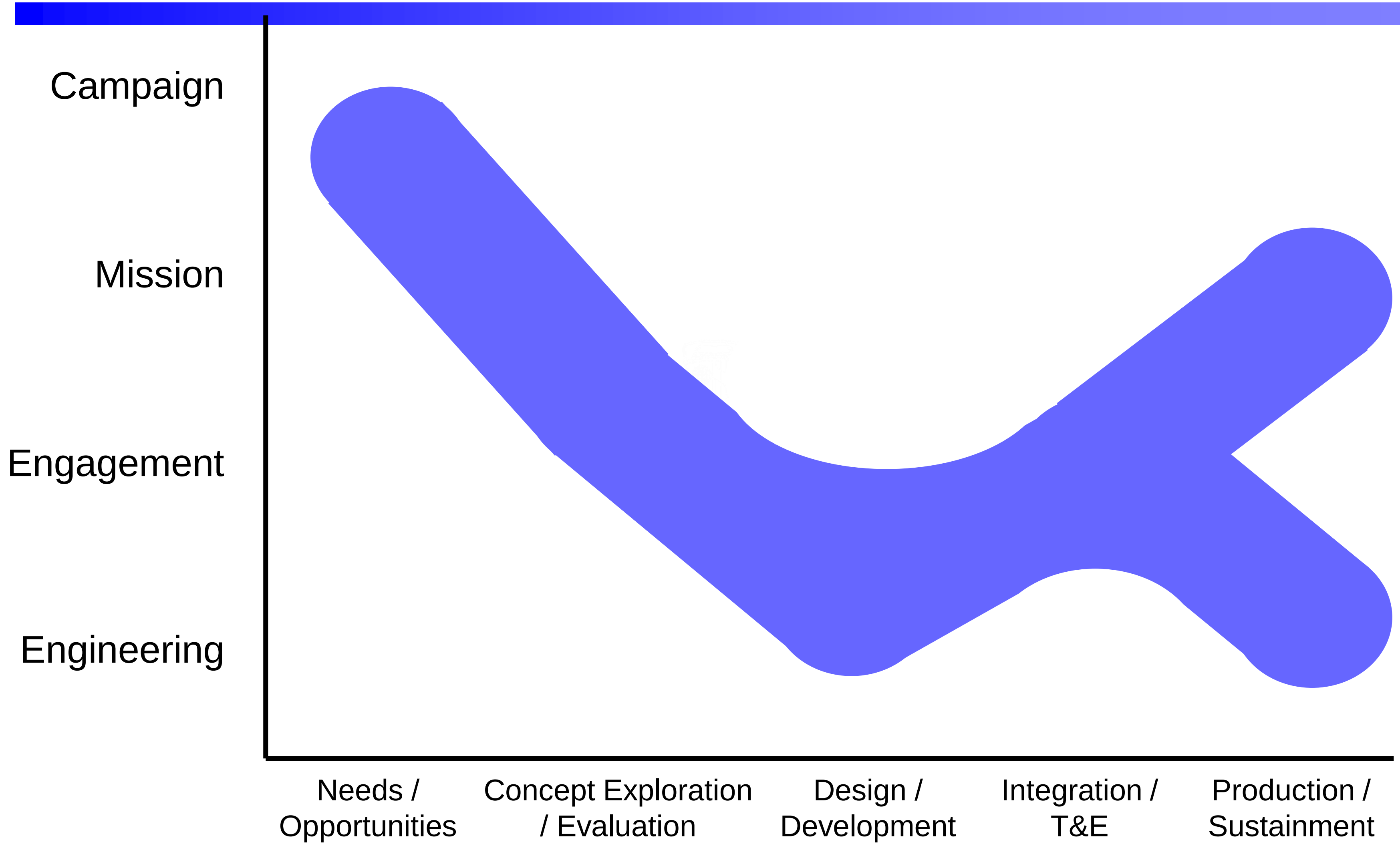
- Production of a hardware system must be planned well in advance, using models and simulations of facilities and processes
- Sustainment (operations and support) costs are usually the largest element of the ownership cost for major military systems
- Progress is being made in the development of standards for models and simulations used for production
- System operation simulations are useful for troubleshooting problems with systems operating in a remote environment
- Process modeling tools are important for both production and sustainment
- Reliability models can be quite complex for major systems
- System cost models need to consider the cost of all elements associated with the ownership of a system

Typical Simulation Resolution Levels During Phases of the Systems Engineering Process



•

Typical Simulation Resolution Levels During Phases of the Systems Engineering Process



•

Selected Detailed Examples (as time permits)

- System Effectiveness Simulation Examples
  - Conceptual model for a communications system
  - Logical data model for a scenario
- Interacting Simulation Examples
  - A Crisis Management and Evacuation System
  - A Mobile Missile System
- Integration and T&E Examples
  - Construction of a Simulation Environment for an Underwater Vehicle's Navigation and Sensor Data Systems
  - Construction of the M&S Portions of a Test and Evaluation Master Plan (TEMP)
- Repair Process for a Deployed Military System Component

System Effectiveness Simulation Example – Conceptual model for a communications system (1 of 4)

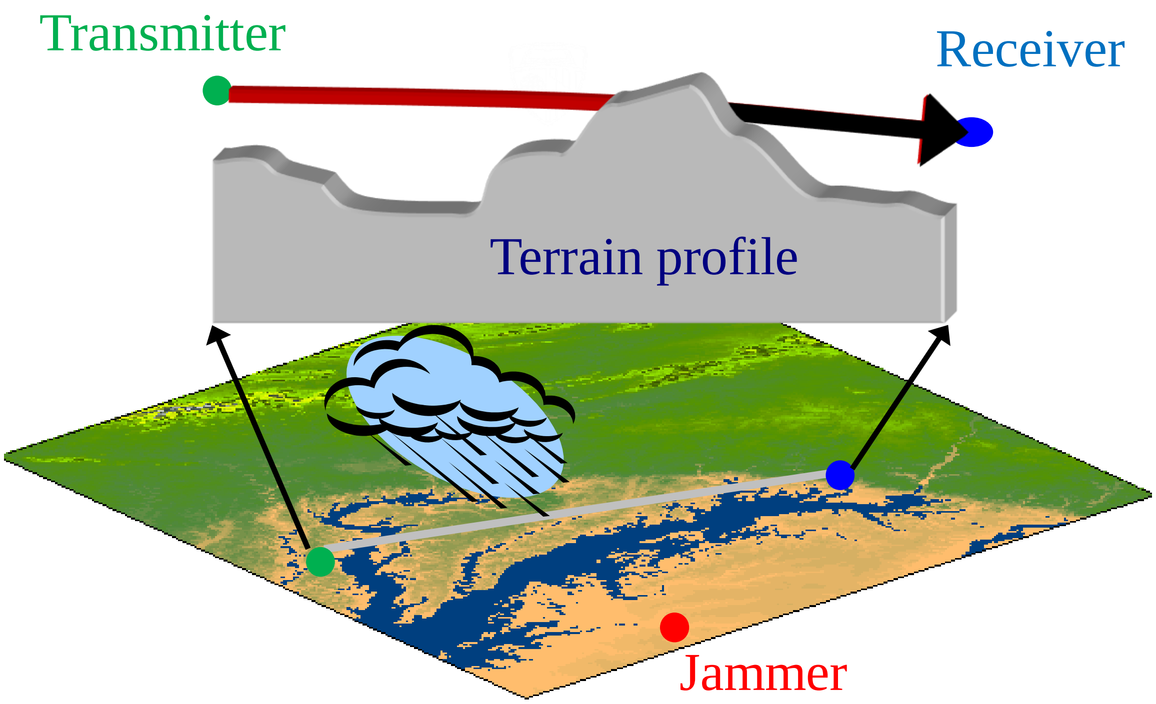
- Question to be answered – how effective would a new radio frequency communications system be in a varied-terrain environment, in the possible presence of rain, with the possibility of jamming by an adversary?
- Develop a simulation conceptual model in graphical form
- What modeling and simulation components/elements are required?
  - Digital Terrain Elevation Data (DTED) for area of interest
  - Initial location and movement scripts for source, receiver, and jammer
  - Rain movement as a function of time
  - Probability of successful communication vs. distance in a benign line-of-sight environment
  - Degradation of probability of successful communication as a function of:
    - Distance of propagation through rain
    - Distance and azimuth of jammer relative to source and receiver
  - Other?

System Effectiveness Simulation Example – Conceptual model for a communications system (2 of 4)

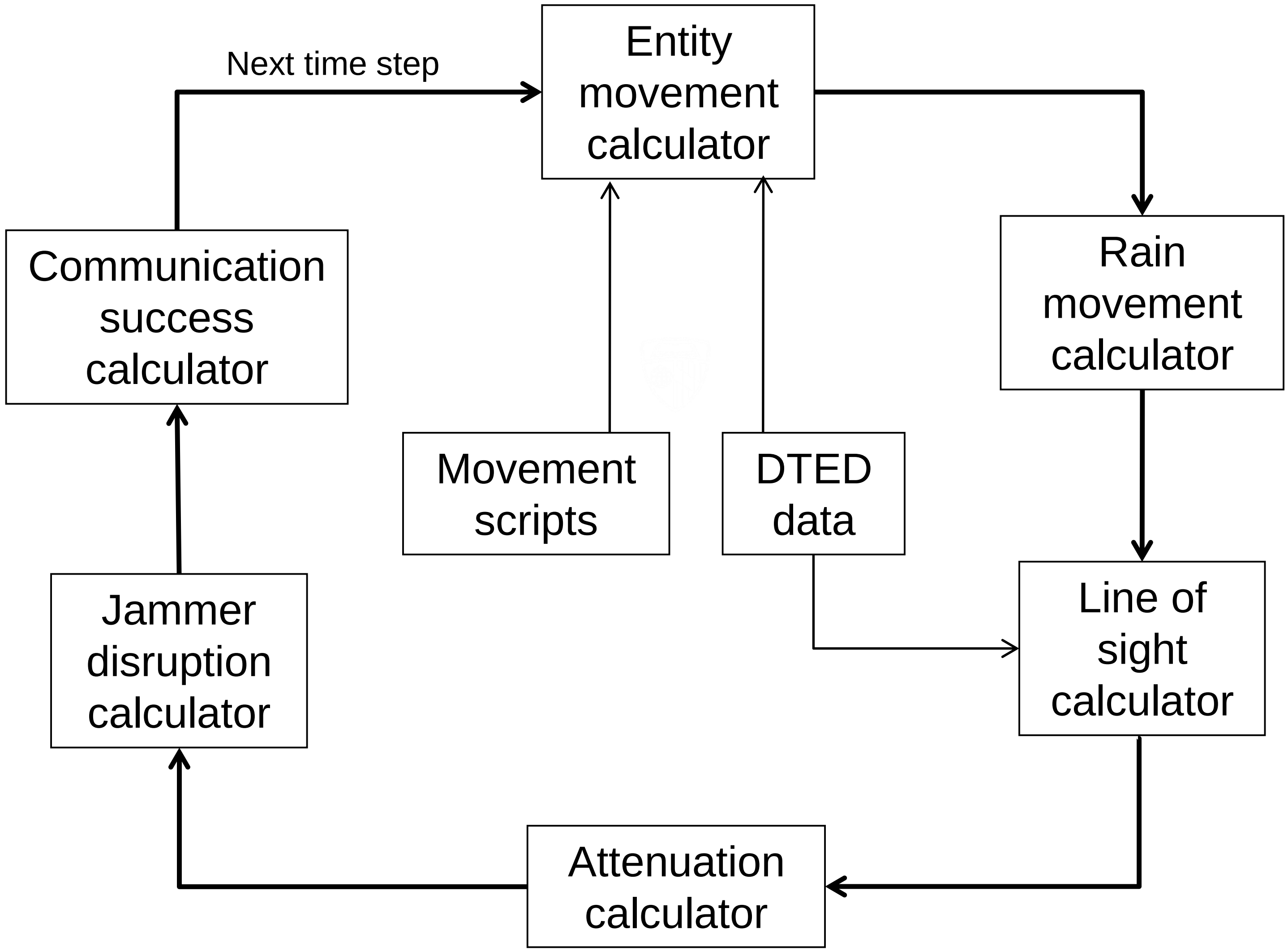
- Measure of effectiveness
  - Probability of successful receipt of a message in a (set of) representative operational environment(s)
- The system representation (in performance terms)
  - Source characteristics (frequency range, power levels, directionality)
  - Receiver characteristics (frequency range, sensitivity, directionality)
- The system's concept of operations
  - Rules on variations in power level selections and antenna pointing angle by operator
- The representation of threats and friendly systems
  - Jammer source characteristics (frequency range, power levels, directionality)
- The representation of the natural and man-made environment
  - DTED data (level 2)
  - Rain effects (attenuation by frequency range and rain density)

System Effectiveness Simulation Example – Conceptual model for a communications system (3 of 4)

- The scenario
  - Movement scripts for source, receiver, and jammer
  - Rain density, expanse, and movement vs. time



System Effectiveness Simulation Example – Conceptual model for a communications system (4 of 4)



System Effectiveness Simulation Example – Logical data model for a scenario

- A time of year and duration
- Location and extent of the play box(es)
  - Example: coordinate sets
- Instantiations of the natural and/or man-made environment
  - Example: environment sets
- The numbers and types of assets (system-of-interest, friendly, threat, neutral)
- System concepts of operation, and the way in which assets move
  - Example: scripted way points

System Effectiveness Simulation Example – Logical data model for a scenario – Scenario identification

- Scenario ID
- Title
- Objective
- Author
- Date
- Start time (GMT)
- End time (GMT)
- Time step

System Effectiveness Simulation Example – Logical data model for a scenario – Coordinate sets

- Coordinate sets may be expressed as multiple X-Y-Z or Lat-Lon-Alt points, in some reference frame, to define an area of interest (e.g., DTED region, play box, etc.)
- Coordinate set ID
- Coordinate set type (X-Y-Z or Lat-Lon-Alt)
- Reference frame (e.g., WGS 1984, UTM)
- Number of coordinate points
- For coordinate sets of type X-Y-Z:
  - Units
  - For each coordinate point:
    - X
    - Y
    - Z
- For coordinate sets of type Lat-Lon-Alt:
  - Lat-Lon units
  - Alt units
  - For each coordinate point:
    - Lat
    - Lon
    - Alt

System Effectiveness Simulation Example – Logical data model for a scenario – Environment sets

- Environment sets can used to describe the environment (land, air, sea) in an area of interest
- Environment ID
- Coordinate set ID reference
- For air environments:
  - Air parameters (e.g., cloud cover density)
- For sea environments:
  - Sea parameters (e.g., sea state)
- For land environments:
  - Land parameters (e.g., terrain height)

System Effectiveness Simulation Example – Logical data model for a scenario – Assets

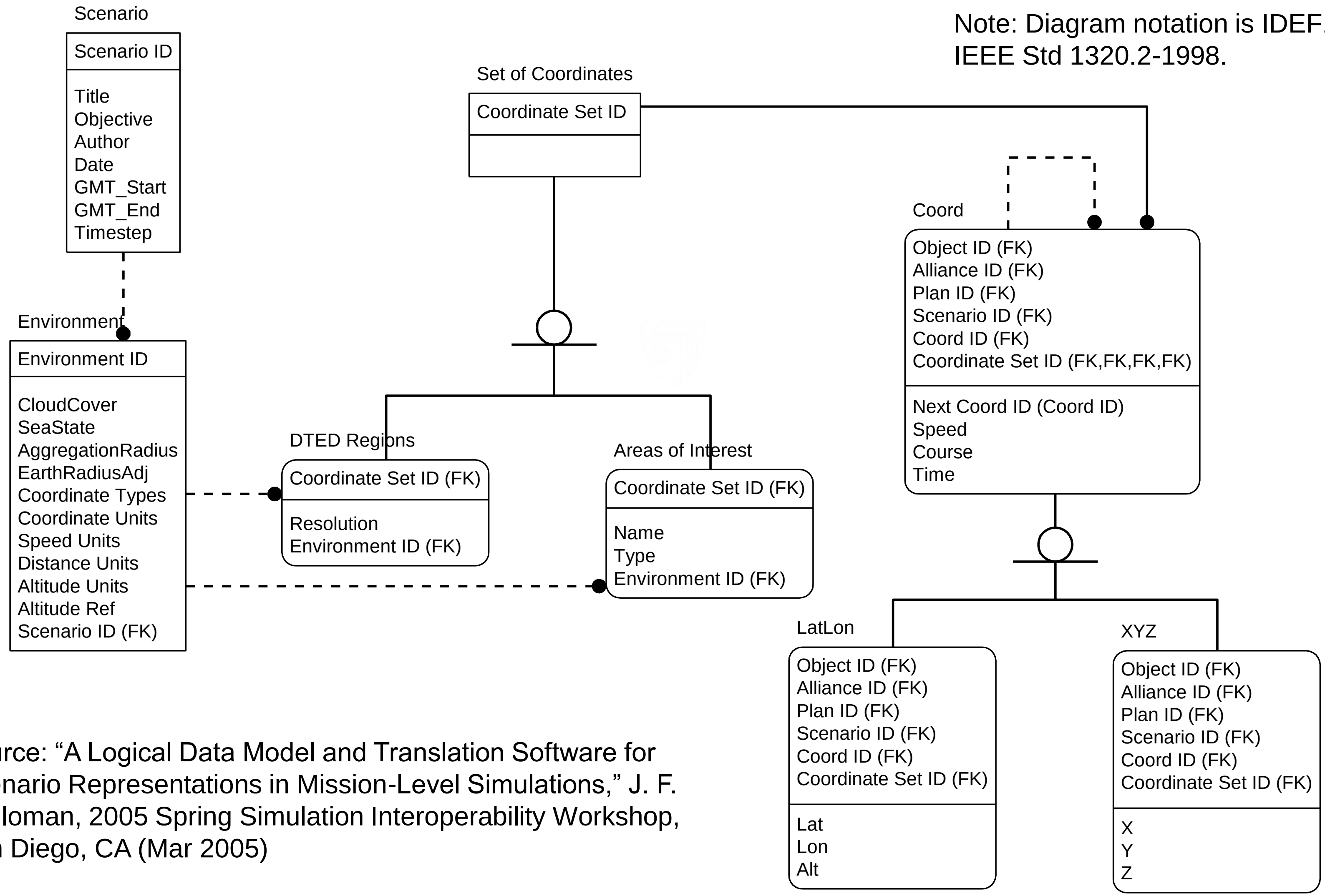
- Assets may be of a number of different types, and may be in alliances with other assets, with the alliances related as friendly, hostile, or neutral
- For each asset:
  - Asset ID
  - Asset classification (e.g., vehicle, command post, sensor)
  - Asset category, within classification (e.g., ship, radar)
  - Alliance ID reference
- For each alliance:
  - Alliance ID
  - Alliance name
  - Alliance asset IDs
- Alliance relationships – for each relationship:
  - Alliance type (friendly, hostile, or neutral)
  - “Subject” alliance ID
  - “Predicate” alliance ID

System Effectiveness Simulation Example – Logical data model for a scenario – Asset movement

- Asset movement in a scenario may be scripted, by specifying a series of way-points and times, or by specifying a series of courses, speeds, and durations
- Way-point movement plan – for each movement:
  - Current coordinate set ID reference
  - Next coordinate set ID reference
  - Arrival time at next coordinate set (assume constant course and speed)
- Course-speed-duration movement plan – for each movement:
  - Course for movement (assume constant)
  - Speed for movement (assume constant)
  - Duration of movement

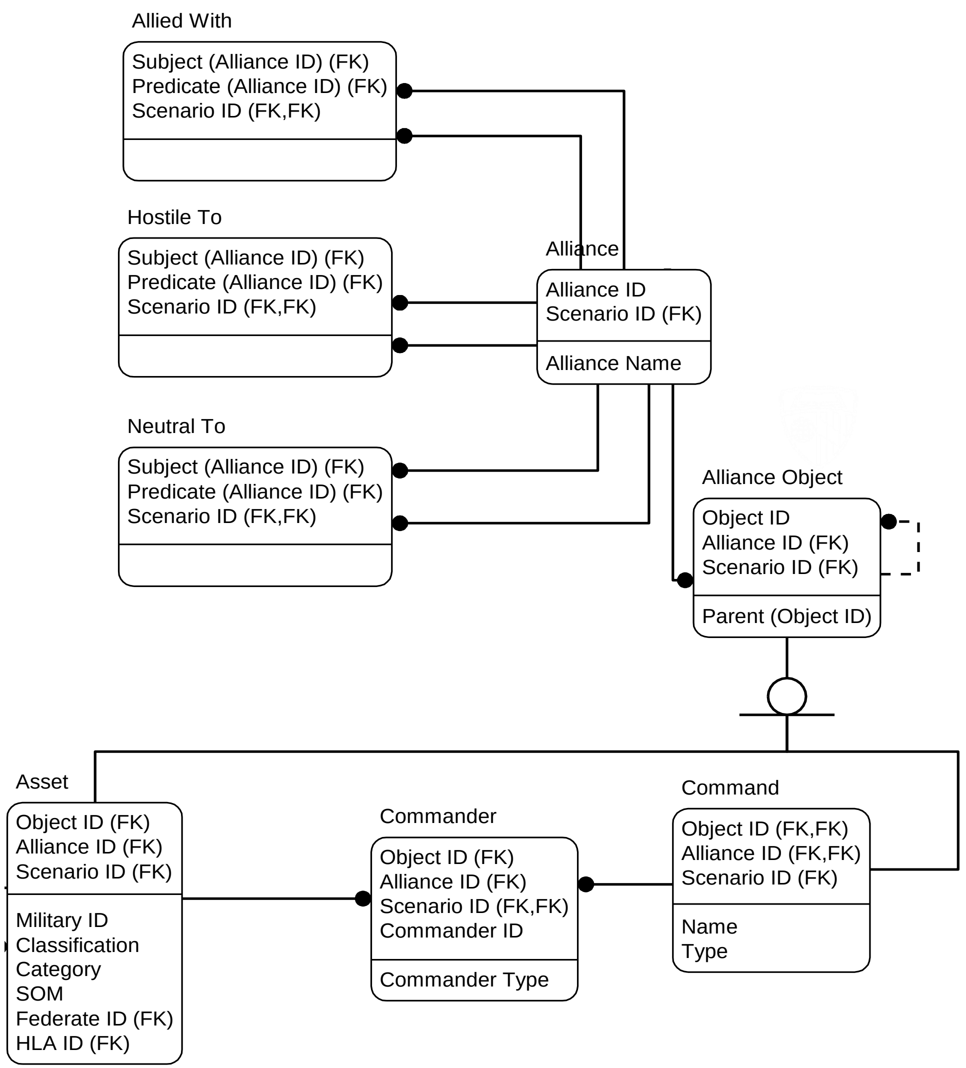
Example of Scenario, Play Boxes, Environment Sets, and Coordinate Sets Relationships

Note: Diagram notation is IDEF1X, IEEE Std 1320.2-1998.



Source: "A Logical Data Model and Translation Software for Scenario Representations in Mission-Level Simulations," J. F. Schloman, 2005 Spring Simulation Interoperability Workshop, San Diego, CA (Mar 2005)

Example of Asset Relationships



Note: Diagram notation is IDEF1X, IEEE Std 1320.2-1998.

Source: “A Logical Data Model and Translation Software for Scenario Representations in Mission-Level Simulations,” J. F. Schloman, 2005 Spring Simulation Interoperability Workshop, San Diego, CA (Mar 2005)

Example: Interacting Simulations for a Crisis Management and Evacuation System

- Design layout of a chemical sensor system for a downtown urban area, and a traffic management system for evacuation during a crisis
- Component Simulations
  - Explosive detonation causing railcar rupture
  - Chemical source strength simulation
  - Chemical plume dispersion simulation
  - Chemical sensor simulation
  - Emergency management command and control simulation
  - Traffic flow simulation

Interacting Simulations for a Crisis Management and Evacuation System – Scenario Use Case

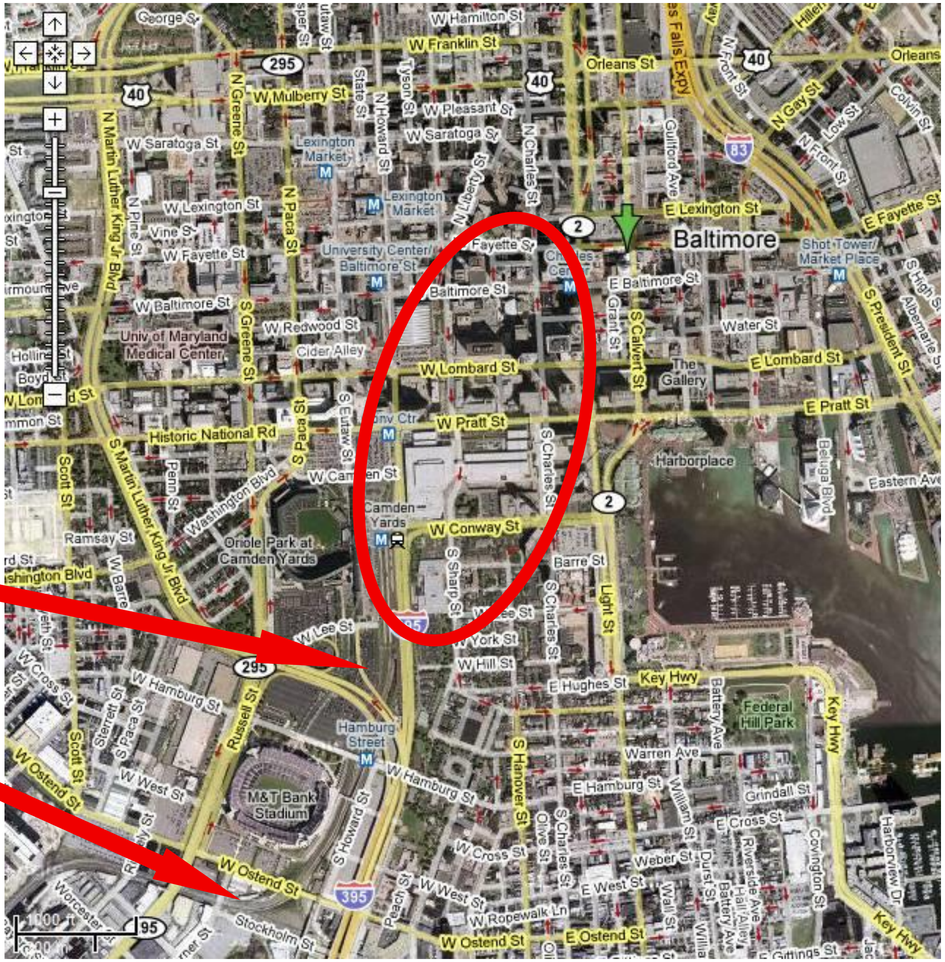
5. Emergency responders react

4. Chlorine cloud moves toward downtown

3. Second explosion, 15 minutes later

2. First explosion

1. Train with railcars containing chlorine approaches



Source: GoogleEarth

6. News reports issued

7. Local commanders order evacuation

8. Police in protective gear dispatched to intersections

9. Chemical sensors deployed

10. Local populace reacts, traffic builds on roads

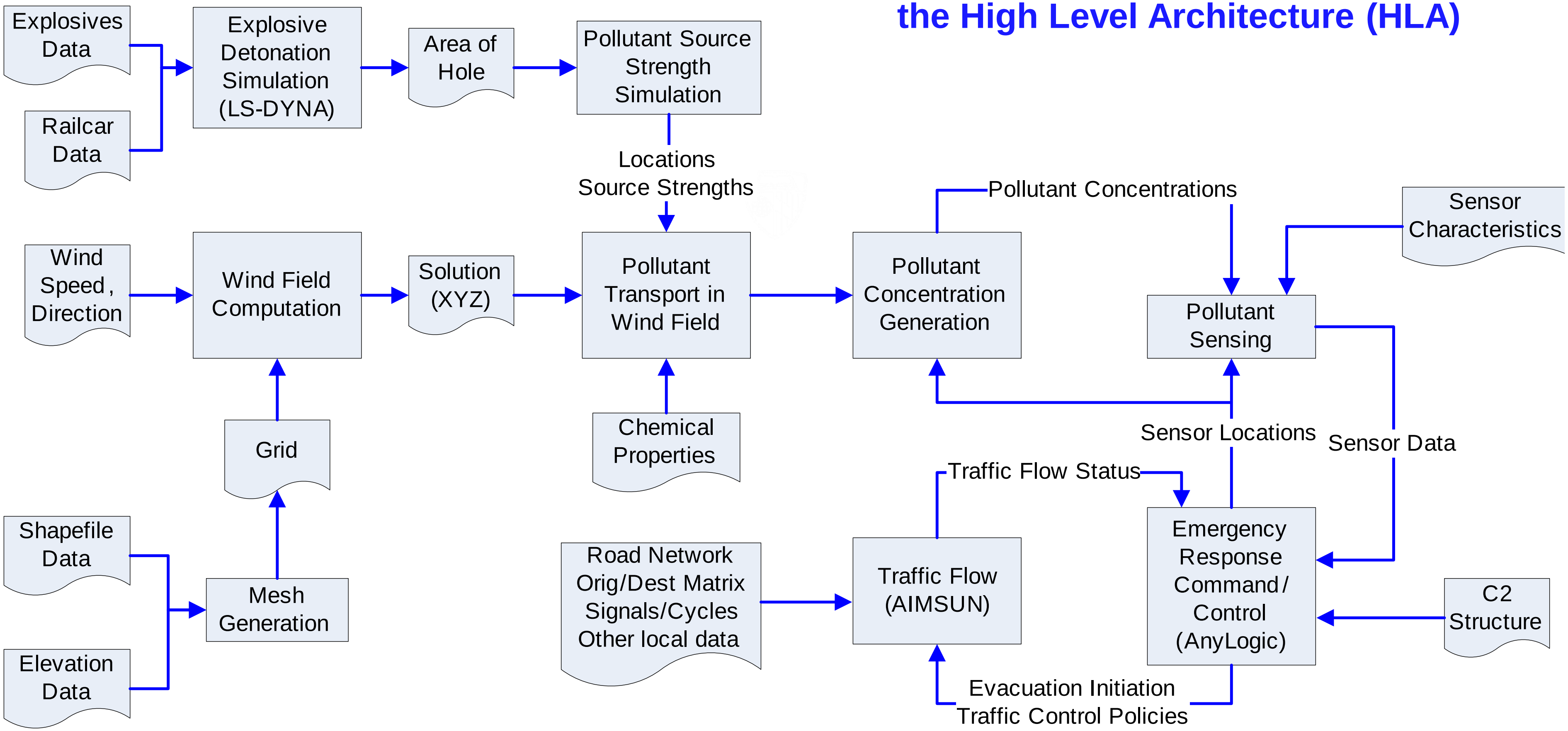
Interacting Simulations for a Crisis Management and Evacuation System – Design Considerations

- Railcar rupture simulation component
  - Needs no feedback from other simulation components
  - Can be executed in advance
- Simulation of airborne transport through 3D cityscape
  - Requires many processors, cannot run in real time – 3 steps:
    - Generation of wind field (slower than real time)
    - Insertion of pollutant into wind field (slower than real time), forming data file of chlorine concentrations
    - Extraction of chlorine concentrations in real time from data file
- Airborne transport depends on release rate of chlorine
  - So chlorine release simulation, although not computationally intensive, needs to be executed in advance
- Remaining three functions (sensing, command and control, and traffic flow) can be performed in real time (or faster) as part of simulation federation

Interacting Simulations for a Crisis Management and Evacuation System – Block Diagram

Non-Real-Time Simulation Components

Real-Time Simulation Federation Components – Federated Using the High Level Architecture (HLA)

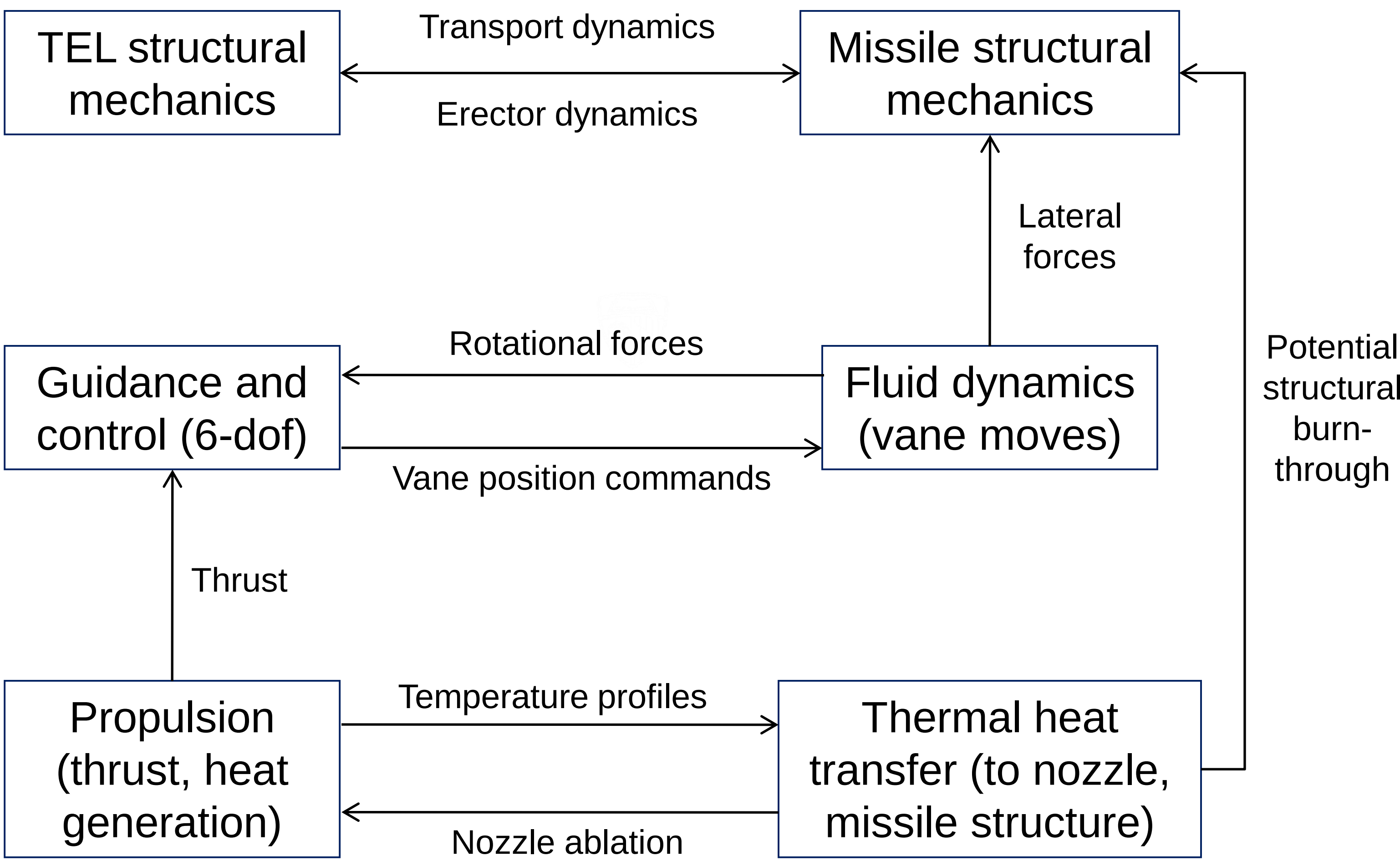


Example: Interacting Simulations for a (Mobile) Missile System

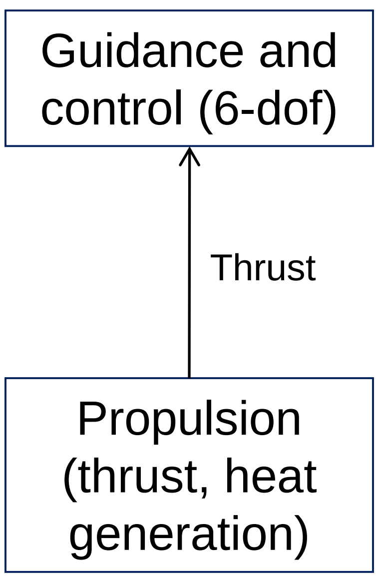
- Simulations of Interest
  - Transporter-Erector-Launcher – Structural Mechanics
  - Missile structure – Structural Mechanics (During Transport and Flight)
  - Propulsion – Thrust, Heat Generation
  - Thermal – Heat Transfer to Nozzle and Missile Structure
  - Guidance and control – 6-dof Flight Simulation
  - Fluid dynamics – Vane Control Effectiveness

Pershing 1A missile (Source: U.S. Army)

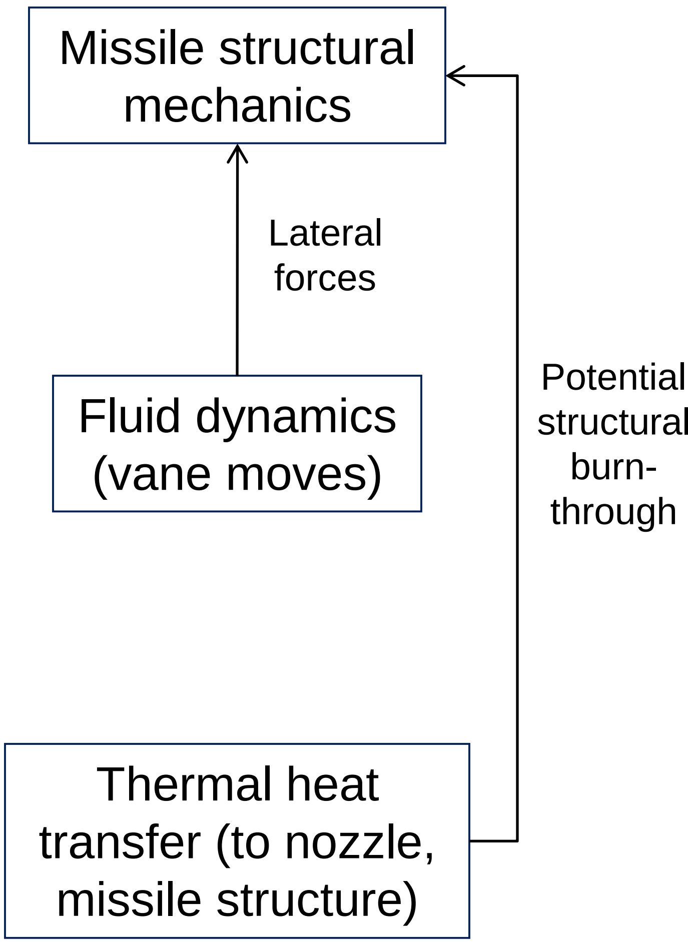
Interacting Simulations for a (Mobile) Missile System: Step 1: Where might there be interactions?



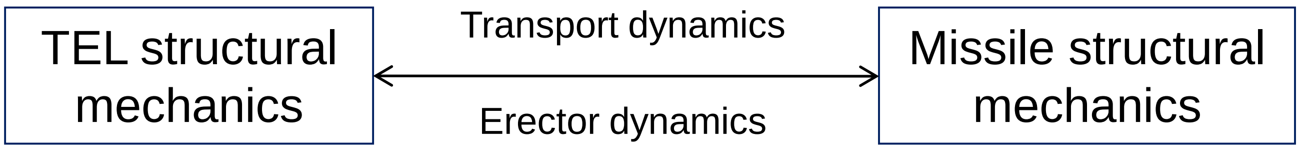
Interacting Simulations for a (Mobile) Missile System: Step 2: Are the interactions one-way or two-way? (1 of 4)



- Interactions between Propulsion and Guidance and control are one-way, during each missile stage's burn time.
- Thermal heat transfer to Missile structure and Vane control to Missile structure are one-way.
- For these, simulations of the first can be run to completion, and their outputs input to simulations of the second. ("Batch runs" can be used.)



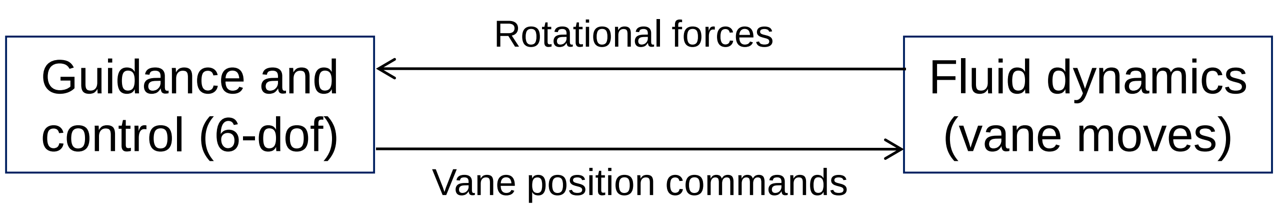
Interacting Simulations for a (Mobile) Missile System: Step 2: Are the interactions one-way or two-way? (2 of 4)



- Pre-launch dynamics between the TEL and the missile are two-way:
  - During transport, the missile and TEL cradle interact in a relatively static configuration
  - When the erector is activated, the missile and TEL erector cradle interact dynamically
- As the concern is structural mechanics for both the missile structure and the TEL, a unified (tightly coupled) structural mechanics simulation of both can be constructed

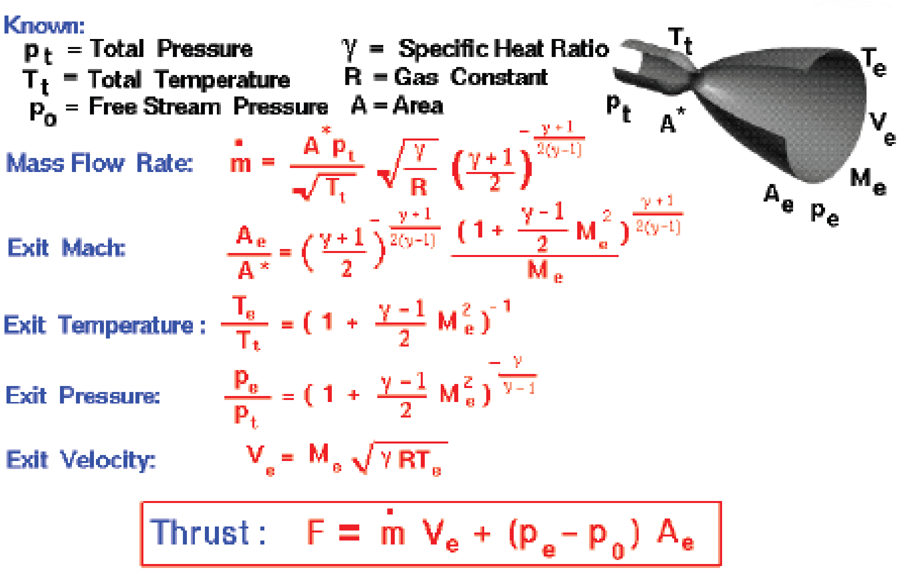
Interacting Simulations for a (Mobile) Missile System: Step 2: Are the interactions one-way or two-way? (3 of 4)

- The interactions between Guidance and control and Fluid dynamics of vane movements are two-way
  - Vane position commands cause vane movement
  - Vane movement produces rotational forces on the missile
- Usually, simulations (computational fluid dynamics codes or wind tunnel tests) are run in advance to calculate rotational forces as a function of vane position, missile angle of attack, and relative velocity
  - This permits the calculation of rotational forces to be embedded in the Guidance and control simulation
- For complex interactions, the Guidance and control and Fluid dynamics of vane movement could be in separate simulations that interchange data during run-time

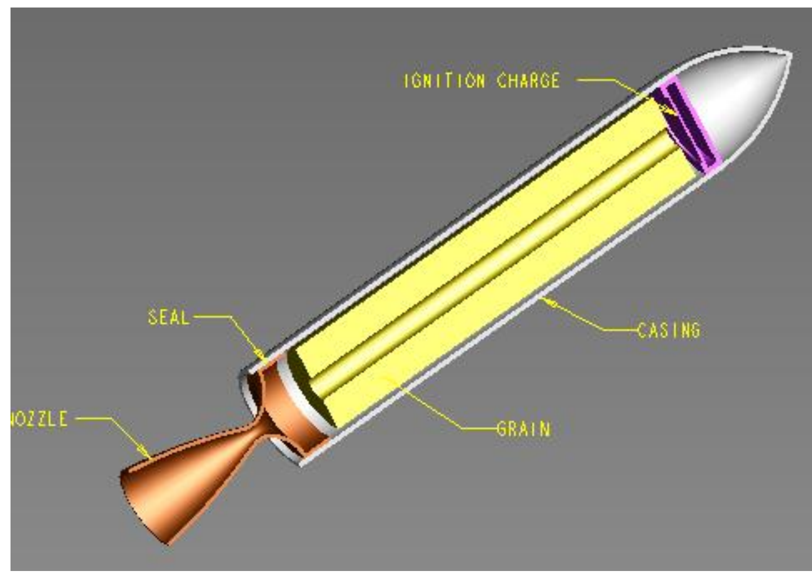


Interacting Simulations for a (Mobile) Missile System: A few basics on solid rocket propulsion and nozzles

- After ignition, solid fuel burns radially out from center toward motor casing
- Fuel burn creates hot gases that exit through nozzle, creating thrust
- Thrust depends on many factors, including nozzle throat area
- Nozzle lining ablates over time, slightly increasing nozzle throat area



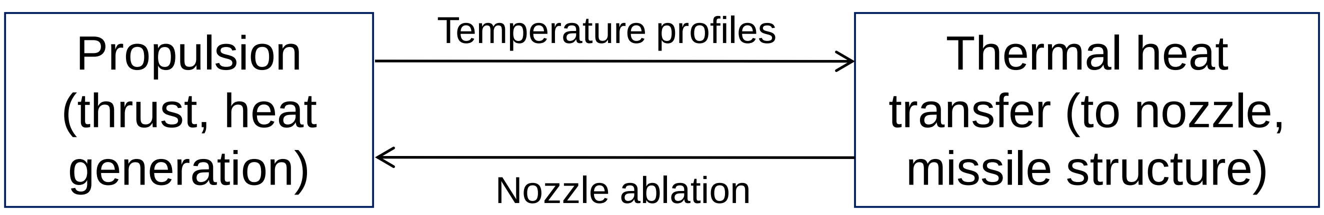
Solid rocket motor thrust equations (source: NASA)



Solid rocket motor (source: Wikipedia Commons)

Interacting Simulations for a (Mobile) Missile System: Step 2: Are the interactions one-way or two-way? (4 of 4)

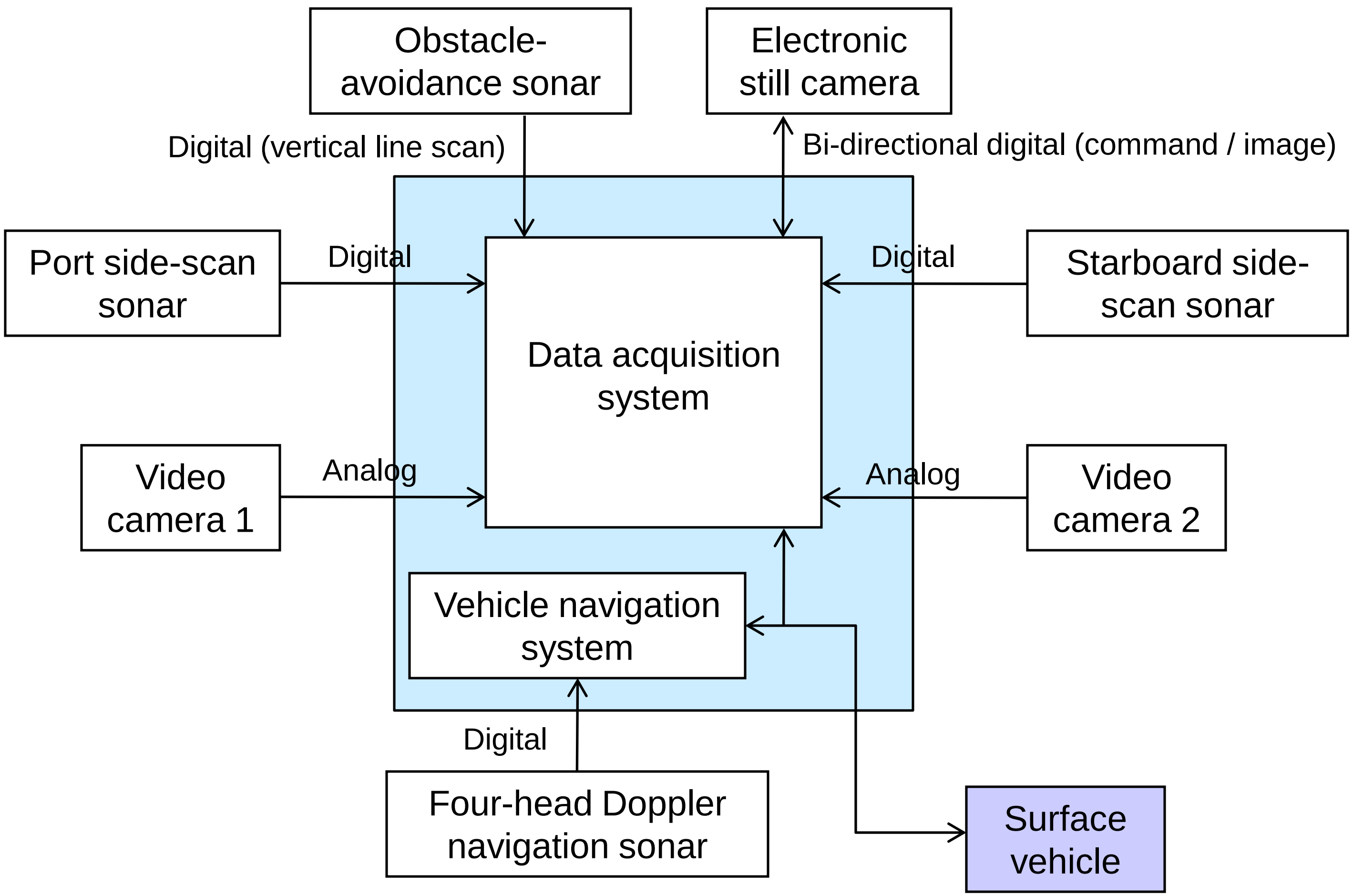
- The interactions between Propulsion and Thermal heat transfer are two-way, because exit gas temperature causes ablation at nozzle throat
- Because of complexity of interactions, for detailed calculations of thrust vs. time, would want to have Propulsion and Thermal heat transfer simulations interact at run-time



Example: Construction of a Simulation Environment for an Underwater Vehicle's Navigation and Sensor Data Systems

- Consider the integration of a tethered underwater vehicle's navigation and sensor systems
- The vehicle will include:
  - A forward-looking obstacle-avoidance sonar
  - Two side-scan sonars (one looking left, one looking right)
  - Two downward-looking full-motion video cameras
  - One downward-looking high-resolution electronic still camera
  - A four-head downward-looking Doppler sonar for navigation
- Prior to receiving the above imaging and navigation sensors, how could simulations be used (as stimulators) to prepare for the sensors' integration with the vehicle's navigation and sensor data acquisition systems?

Simulation Environment for an Underwater Vehicle's Navigation and Sensor Data Systems – Potential System Design

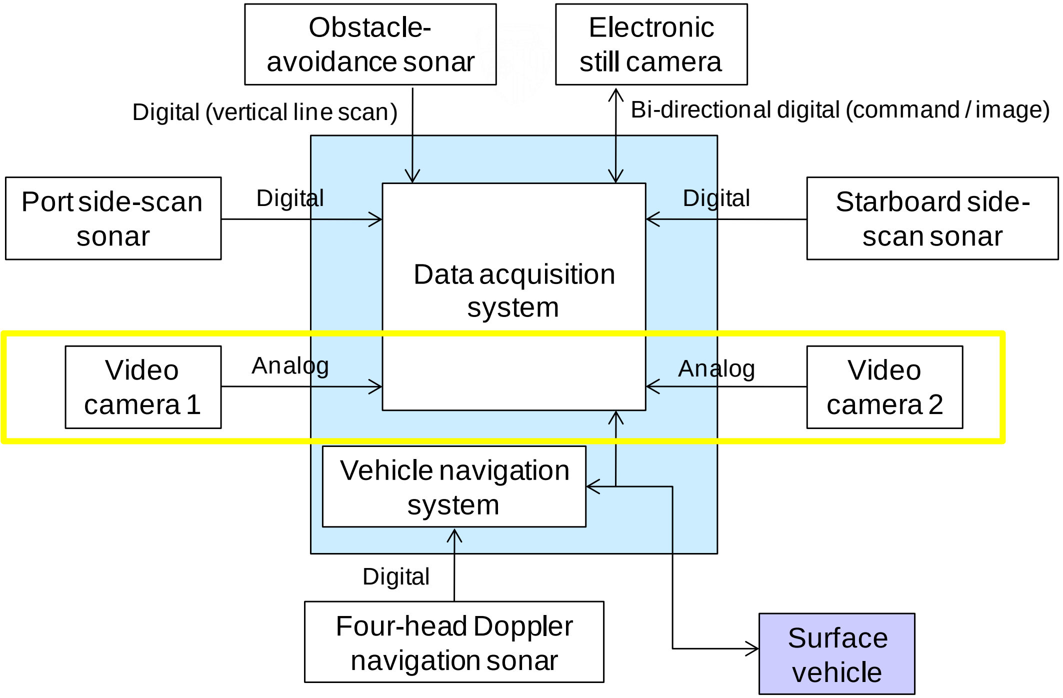


Simulation Environment for an Underwater Vehicle's Navigation and Sensor Data Systems – Considerations

- In the system being built, what are the interfaces between the imaging / navigation sensors and the vehicle's navigation and sensor data acquisition systems?
  - Are the interfaces analog or digital?
  - For analog interfaces, what analog data communication standards are being used (video, acoustic, other)?
  - For digital interfaces:
    - What digital data communication hardware standards are being used (e.g., RS-232, Ethernet, USB)?
    - What data formatting techniques are being used (e.g., XML, byte-ordering scheme, proprietary)?
    - What syntax is being used for the data in each data transmission frame?
    - What is the frame transmission rate?
- To what degree does testing require that simulated data be representative of expected real data?
  - Are only the data rate and data format/syntax important?
  - Do images need to be realistic (e.g., if the data acquisition system employs feature recognition to make a decision)?
  - Does navigation sensor data need to be used to develop a simulated track?

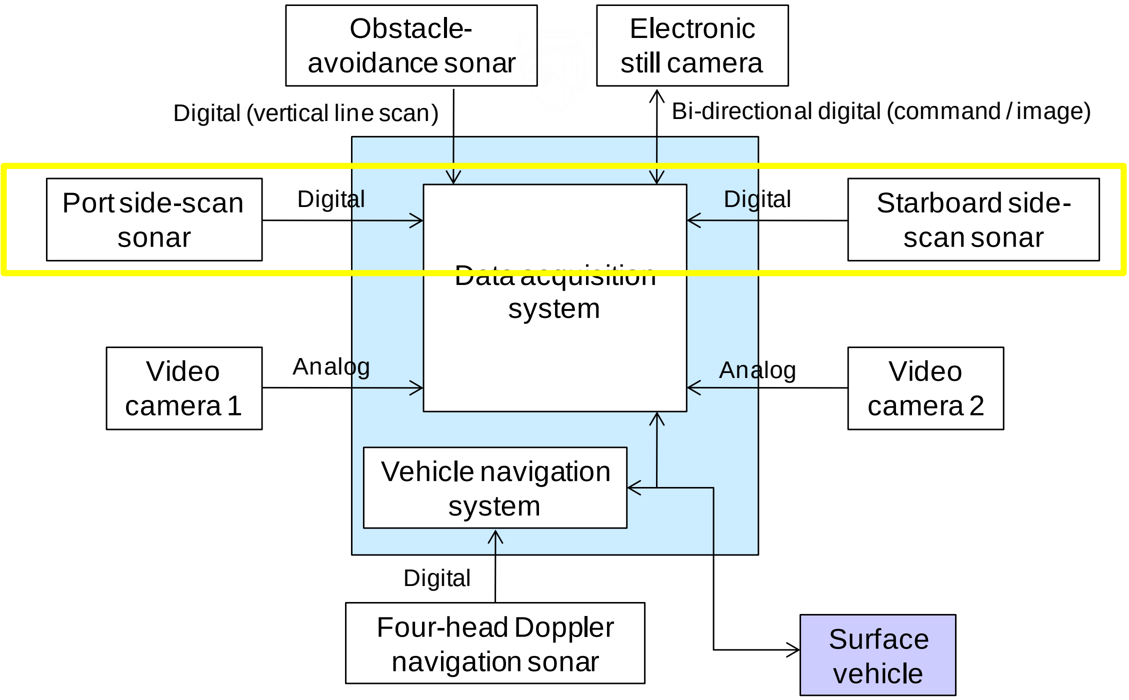
Simulation Environment for an Underwater Vehicle's Navigation and Sensor Data Systems – Video Cameras

- Design note: Analog video camera signals are merely re-transmitted in analog form to the surface vehicle for viewing by operators and possible recording.
- Therefore the video camera simulations (stimulators) can be simple hardware video sources, even VCRs with arbitrary interfaces



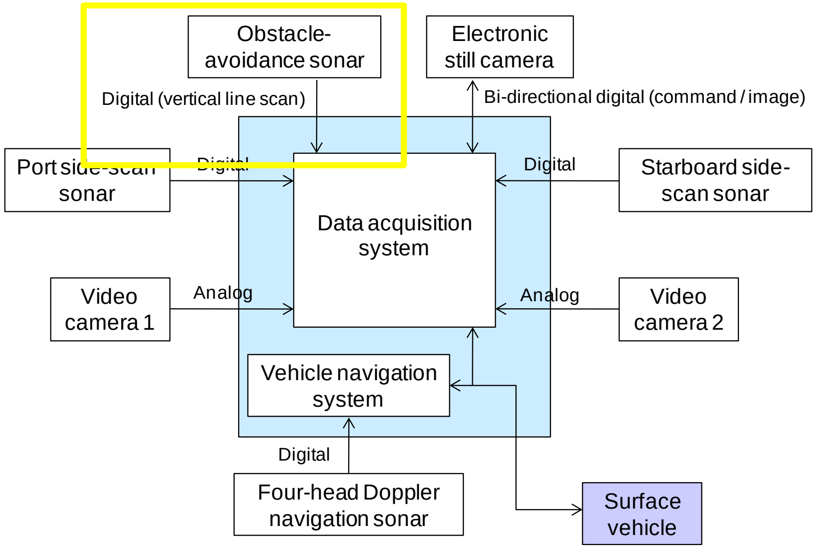
Simulation Environment for an Underwater Vehicle's Navigation and Sensor Data Systems – Side-scan Sonars

- Design note: Each side-scan sonar produces a "line" of 1024 pixels with black-and-white intensity from 0 to 255, once per second; lines are merely re-transmitted to the surface vehicle.
- Therefore the side-scan sonar simulations (stimulators) need only replicate the data rates of the sensors.



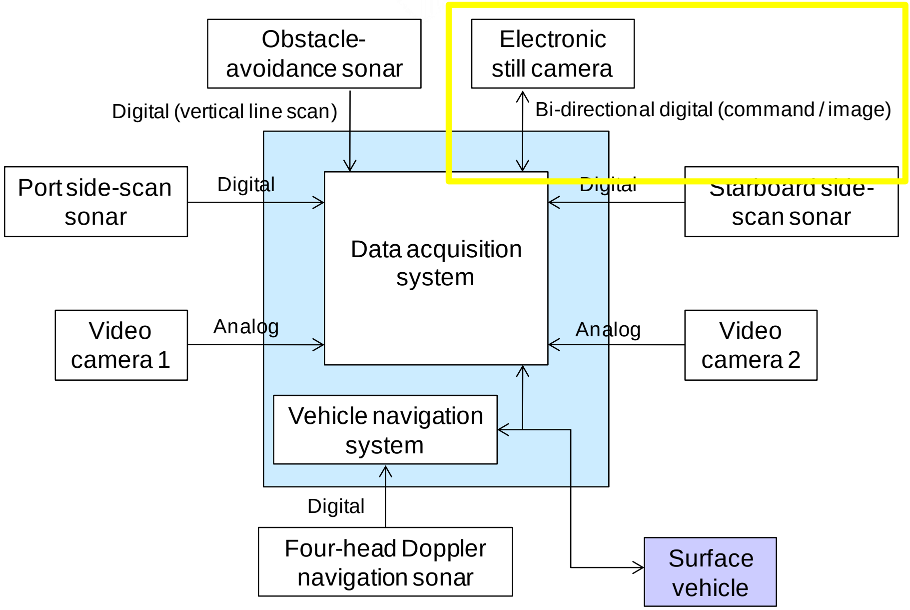
Simulation Environment for an Underwater Vehicle's Navigation and Sensor Data Systems – Obstacle Avoidance Sonar

- Design notes:
  - The obstacle avoidance sonar produces a "vertical line" of 256 pixels (covering a 30-degree vertical field of view) with black-and-white intensity from 0 to 255, 5 times per second, sweeping a 30-degree horizontal field of view in 30 seconds to form a 256x150 continually-updated image.
  - The data acquisition system generates an alarm when a "dark object" of a certain size is in the center of the field of view.
- Therefore the obstacle-avoidance sonar simulation (stimulator) must provide, at the required rate, representative data that will show both no dark objects and an occasional realistic dark object over time.



Simulation Environment for an Underwater Vehicle's Navigation and Sensor Data Systems – Electronic Still Camera

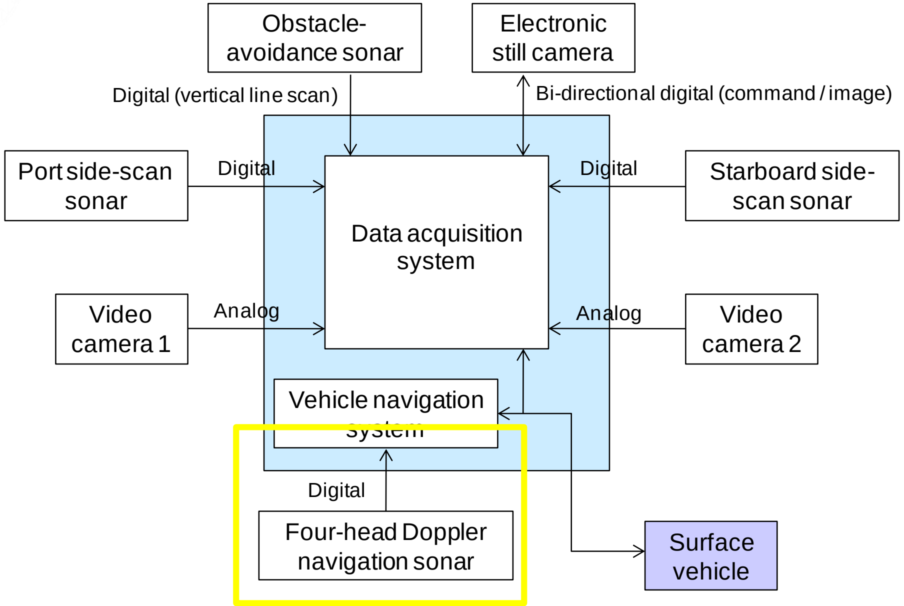
- Design note: The electronic still camera, upon a command from the data acquisition system, takes a single 1024 x 1024 pixel (with black-and-white intensity from 0 to 255), at a maximum rate of once per second. Images are merely re-transmitted to the surface vehicle.
- Therefore the electronic still camera simulation (stimulator) needs to replicate the data rate (up to 8 megabits per second) and pixel transmission order of the camera, upon receipt of a command.



Simulation Environment for an Underwater Vehicle's Navigation and Sensor Data Systems – Doppler Nav Sonar

- Design note: The Doppler navigation sonar transmits four digital values (from 0 to 4095), once per second, representing fore, port, aft, and starboard speeds relative to the bottom of the body of water. The vehicle navigation system uses these values to compute an instantaneous vehicle velocity and to produce a continuous x-y track relative to the bottom.

- Therefore the Doppler navigation sonar simulation (stimulator) needs to provide an operationally realistic (within vehicle propulsion capabilities), time-consistent (second-to-second) set of four speed values to the vehicle navigation system).



Example: Construction of the M&S Portions of a Test and Evaluation Master Plan (TEMP)

- Consider a Test and Evaluation Master Plan for a ballistic missile interceptor missile, which could include descriptions of such T&E activities as
  - Subsystem tests of radar seeker
  - Subsystem tests of focal plane array
  - Wind tunnel tests using scaled missile model
  - Static tests (on test stand) of propulsion subsystem
  - Flight tests on a test range
  - Post-flight evaluation
- What types of models and simulations are needed for each T&E activity?
  - Where might simulations be used? Where might models be used?
  - For the simulations, which are live? Which are virtual? Which are constructive?

Extracts from DoD Instruction 5000.02 Regarding Test and Evaluation Master Plan (TEMP)

- Test and Evaluation Master Plan (TEMP). … The TEMP shall describe planned developmental, operational, and live-fire testing, including measures to evaluate the performance of the system during these test periods; an integrated test schedule; and the resource requirements to accomplish the planned testing. …
  - (6) Appropriate use of accredited models and simulation shall support DT&E, IOT&E, and LFT&E.

DT&E: Developmental Test & Evaluation
OT&E: Operational Test & Evaluation
LFT&E: Live Fire Test and Evaluation

Source: DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, December 8, 2008

References to Modeling and Simulation in Recommended TEMP Format

- **PART III – TEST AND EVALUATION STRATEGY**
  - 3.3 DEVELOPMENTAL EVALUATION APPROACH
    - 3.3.3 Modeling and Simulation
  - 3.4 LIVE FIRE EVALUATION APPROACH
    - 3.4.2 Modeling and Simulation
  - 3.6 OPERATIONAL EVALUATION APPROACH
    - 3.6.2 Modeling and Simulation
- **PART IV – RESOURCE SUMMARY**
  - 4.1 INTRODUCTION
    - 4.1.7 Models, Simulations, and Test-beds

Source: Annex to *Defense Acquisition Guidebook*, Section 9.10, "Test and Evaluation Master Plan (TEMP) Recommended Format"

Developmental Test & Evaluation: Tests of Interceptor Sensor Subsystems

- Radar seeker subsystem testing
  - Intended to estimate performance of the in-development seeker
  - Employs hardware-in-the-loop (HWIL) simulation
    - Radar seeker is a live simulation component (the real seeker)
    - Target object in an anechoic chamber is a constructive simulation component (a simulation of a potential target)
- Focal plane array subsystem testing
  - Intended to estimate performance of the in-development array
  - Employs HWIL simulation
    - Focal plane array is a live simulation component (the real array)
    - Target representation is a constructive simulation component (e.g., an array of light-emitting devices representing various target and background signatures)
  - May also have a software-in-the-loop (SWIL) component
    - Image processing software embedded in seeker system for target recognition and discrimination

Developmental Test & Evaluation: Aerodynamic and Propulsion Testing

- Wind tunnel testing using scaled missile model
  - Intended to estimate aerodynamic performance of missile at various speeds and angles of attack
  - Employs a physical model of the missile body
  - Wind tunnel test itself is a simulation
    - Wind field is a constructive environmental simulation component (of the real relative wind the missile would see during actual flight)
- Static testing (on test stand) of propulsion subsystem
  - Intended to estimate thrust vs. time of the missile interceptor
  - Employs HWIL simulation
    - Missile stage containing propellant and ignition system is a live simulation component (the real missile stage)

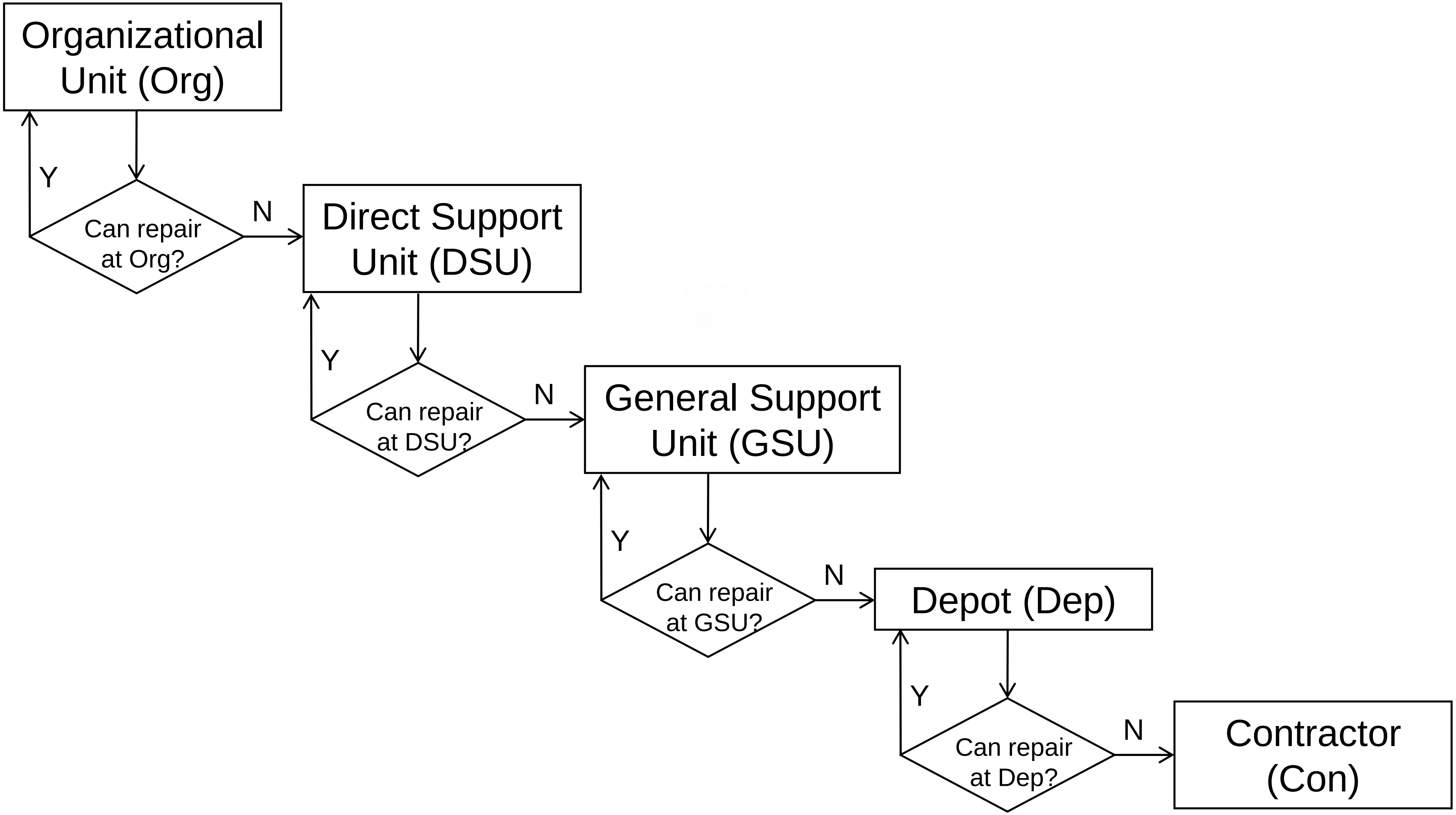
DT&E and OT&E (Potentially Combined): Flight Tests and Post-Flight Evaluation

- Flight test on a test range
  - Intended to measure interceptor performance in varied realistic conditions
  - Pre-flight predictions are done using constructive six-degree-of-freedom (6-dof) simulations (for test design and range safety purposes)
  - For flight test itself
    - Interceptor and target missile are live simulation components
    - If interceptor launch is under operator control, the operator is a live simulation component
- Post-flight evaluation
  - Intended to evaluate single- and multiple-flight test performance
  - Post-flight "predictions" (e.g., using actual wind conditions) are often done using 6-dof simulations (for comparison to telemetry data)
  - Using multiple-flight data, can use data to create better model of interceptor guidance and control system (e.g., using Kalman filtering approach)

Example: Repair Process for a Deployed Military System Component

- Consider the repair process for a deployed military system component (radio) associated with a communications van in theater
  - When the radio malfunctions, what is the initial repair process?
  - If the radio cannot be fixed in place, where does it go?
  - How many levels of repair are implemented?
  - What is the spare parts strategy and inventory?
- How would you model the repair process using a tool such as Arena?

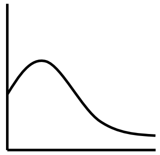
Example Levels/Sequence of Repair



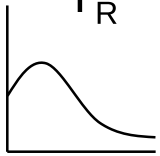
Modeling the Repair Process

- Each possible point of repair has a probability that the radio can be repaired there
  - If it can be repaired there, there is a distribution of repair times
  - If it cannot be repaired there:
    - There is a distribution of times it takes to come to that decision
    - There is a transportation time to the next level of repair

P_R

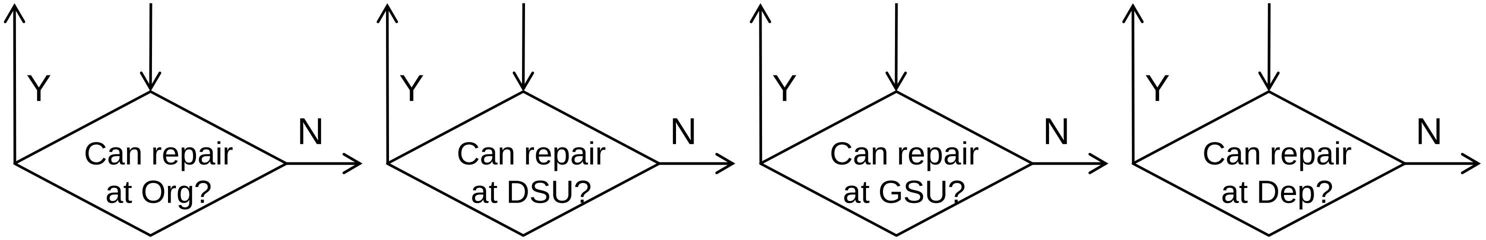


T_R



T_D

T_T



Modeling the Repair Parts Supply Chain

- Modeling Issues
  - Based on reliability models, how many of each radio part should be stored at each repair point?
  - When a spare part is used at a repair point, from where is a replacement requested?
  - Based on reliability/availability models and logistics/transportation cost issues, at what spare parts inventory level at a given repair point should replacements be shipped?

Organizational Unit (Org)

Direct Support Unit (DSU)

General Support Unit (GSU)

Depot (Dep)

Contractor (Con)

19702
MIL-STD-882E Software System Safety Tutorial

An Approach for Focused and Effective Level of Rigor (LoR)

Stuart A. Whitford
Booz Allen Hamilton
20th Annual NDIA Systems Engineering Conference
Springfield, VA
23 October 2015

Agenda

- MIL-STD-882E Requirements for Software Safety
- DoD Guidance for Software Safety
- Software System Safety Hazard Analysis
- Functional Hazard Analysis (FHA) for Software
- In-Depth Safety-Specific Testing
- Requirements Analysis
- Architecture Analysis
- Design Analysis
- Code Analysis
- Wrap Up

Learning Objectives

Gain an understanding of:

- A framework for performing and documenting MIL-STD-882E-required software safety Level of Rigor (LoR)

NOTE: Blue font is used in these slides to highlight significant terms or statements.

Learning Objectives

Gain an understanding of :

- A framework for performing and documenting MIL-STD-882E-required software safety Level of Rigor (LoR)

NOTE: This framework will NOT be a detailed step-by-step process of exactly how to perform each analysis on every system

Learning Objectives

Gain an understanding of:

- A framework for performing and documenting MIL-STD-882E-required software safety Level of Rigor (LoR)
- How to focus analysis of software requirements and architecture on the command and control of Safety-Significant Functions

Learning Objectives

Gain an understanding of:

- A framework for performing and documenting MIL-STD-882E-required software safety Level of Rigor (LoR)
- How to focus analysis of software requirements and architecture on the command and control of Safety-Significant Functions
- How to focus analyses of the design and code on Safety-Critical Decision Points

Learning Objectives

Gain an understanding of:

- A framework for performing and documenting MIL-STD-882E-required software safety Level of Rigor (LoR)
- How to focus analysis of software requirements and architecture on the command and control of Safety-Significant Functions
- How to focus analyses of the design and code on Safety-Critical Decision Points
- How to derive the safety-specific test cases from the analysis

MIL-STD-882E Requirements for Software Safety

Some MIL-STD-882E Terminology

Software. A combination of associated computer instructions and computer data that enable a computer to perform computational or control functions. Software includes computer programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system. Software includes new development, complex programmable logic devices (firmware), NDI, COTS, GOTS, re-used, GFE, and Government-developed software used in the system.

Software system safety. The application of system safety principles to software.

Some MIL-STD-882E Terminology

Software control category. An assignment of the degree of autonomy, command and control authority, and redundant fault tolerance of a software function in context with its system behavior.

SCC	Software Control Category
SwCI	Software Criticality Index

Level of rigor (LoR). A specification of the depth and breadth of software analysis and verification activities necessary to provide a sufficient level of confidence that a safety-critical or safety-related software function will perform as required.

Some MIL-STD-882E Terminology

Safety-critical. A term applied to a condition, event, operation, process, or item whose mishap severity consequence is either Catastrophic or Critical (e.g., safety-critical function, safety-critical path, and safety-critical component).

Safety-related. A term applied to a condition, event, operation, process, or item whose mishap severity consequence is either Marginal or Negligible.

Safety-significant. A term applied to a condition, event, operation, process, or item that is identified as either safety-critical or safety-related.

Some MIL-STD-882E Terminology

Safety-critical function (SCF). A function whose failure to operate or incorrect operation will directly result in a mishap of either Catastrophic or Critical severity.

SSF	Safety-Significant Function
SSSF	Safety-Significant Software Function

Requirements for Software Safety

[from MIL-STD-882E]

4.1 General. When this Standard is required in a solicitation or contract, but no specific tasks are included, only Sections 3 and 4 apply. The definitions in 3.2 and all of Section 4 delineate the minimum mandatory definitions and requirements for an acceptable system safety effort for any DoD system.

. . .

4.3.2 Identify and document hazards. Hazards are identified through a systematic analysis process that includes system hardware and software, system interfaces (to include human interfaces) . . .

Requirements for Software Safety

[from MIL-STD-882E]

4.4 Software contribution to system risk. The assessment of risk for software, and consequently software-controlled or software-intensive systems, cannot rely solely on the risk severity and probability. . . Therefore, another approach shall be used for the assessment of software's contributions to system risk that considers the potential risk severity and the degree of control that software exercises over the hardware.

Severity Categories

Description	Severity Category	Mishap Result Criteria
Catastrophic	1	Could result in one or more of the following: death . . . or monetary loss equal to or exceeding $10M.
Critical	2	Could result in one or more of the following: permanent partial disability, injuries or . . . monetary loss equal to or exceeding $1M but less than $10M.
Marginal	3	Could result in one or more of the following: injury . . . resulting in one or more lost work day(s) . . . or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	4	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day . . or monetary loss less than $100K.

Software Control Categories

Name	Level	Description
Autonomous (AT)	1	Software functionality that exercises autonomous control authority . . . ***without the possibility of predetermined safe detection and intervention*** **. . .**
Semi-autonomous (SAT)	2	Software functionality that exercises control . . . allowing time for predetermined ***safe detection and intervention by independent safety mechanisms*** **. . .**
Redundant Fault Tolerant (RFT)	3	Software functionality that issues commands . . . ***requiring a control entity to complete the command function*** **. . .**
Influential (INF)	4	Software ***generates information*** of a ***safety-related*** nature used to make decisions by the operator **. . .**
No Safety Impact (NSI)	5	Software functionality that does not possess command or control authority . . . and does not provide safety-significant information **. . .**

Booz | Allen | Hamilton

Software Safety Criticality Matrix

Severity \\ Control	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1 (AT)	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2 (SAT)	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3 (RFT)	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4 (INF)	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5 (NSI)	SwCI 5	SwCI 5	SwCI 5	SwCI 5

NOTE: The Influential (INF) SCC only applies to the generation of 'safety-related' information for the operator.

Software Safety Levels of Rigor

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform *analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing*.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

Safety Risk for Failure to Perform LoR

RELATIONSHIP BETWEEN SwCI, RISK LEVEL, LoR TASKS, AND RISK		
SwCI	Risk Level	Software LoR Tasks and Risk Assessment/Acceptance
1	High	If SwCI 1 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as HIGH . . .
2	Serious	If SwCI 2 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as SERIOUS . . .
3	Medium	If SwCI 3 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as MEDIUM . . .
4	Low	If SwCI 4 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as LOW . . .
5	Not Safety	No safety-specific analyses or testing is required.

DoD Guidance for Software Safety

MIL-STD-882E Guidance for Software Safety

[from Tasks 102 and 103 – System Safety Program Plan and Hazard Management Plan]

102/103.2.6 Hazard analysis.

. . .

i. Describe a systematic software system safety approach to:

. . .

(4) Identify and assign the Software Criticality Index (SwCI) for each safety-significant software function (SSSF) and its associated requirements.

MIL-STD-882E Guidance for Software Safety

[from Task 208 – Functional Hazard Analysis]

208.2.1 . . .

g. An assessment of Software Control Category (SCC) for each Safety-significant Software Function (SSSF). Assign a Software Criticality Index (SwCI) for each SSSF mapped to the software design architecture.

JSSEH Guidance

4.2.1.4 Defining and Using the Software Criticality Matrix

... It is through this prioritization that safety-significant code can receive the appropriate robustness and level of rigor over the lifecycle, while effectively managing the critical resources of the program. The most important aspect of the activity is that the software with the highest level of control over safety-significant hardware must receive more attention or level of rigor than software with less safety risk potential. . .

JSSEH Guidance

4.2.1.4 Defining and Using the Software Criticality Matrix

... It is through this prioritization that safety-significant code can receive the appropriate robustness and level of rigor over the lifecycle, while effectively managing the critical resources of the program. The most important aspect of the activity is that the software with the highest level of control over safety-significant hardware must receive more attention or level of rigor than software with less safety risk potential. . . This methodology helps prioritize and manage the critical resources of schedule, budget, and personnel associated with the development of the system.

JS-SSA Software System Safety:

Implementation Process and Tasks Supporting MIL-STD-882E

3.5. [LoR] Allocations to Safety-Significant Functions

The allocation of SSFs to specific [LoR] categories is essential, both to ensure the provision of rigor to the functions of highest safety criticality and to ensure the management of the critical resources necessary to implement that rigor. . . [T]he accomplishment of the subtasks … must be thoroughly documented within the artifacts of the safety analysis.

Software System Safety Hazard Analysis – an Overview

Where to Focus

14-5.c. ... focus ... on hazard identification and mitigation of software causal factors, as opposed to error removal.

14-5.d. ... focus … on hazard and software causal factor identification and mitigation, as opposed to requirements perfection. [Software safety requirements should be based on mitigating software related hazards.]

NAVSEA SW020-AH-SAF-010, Section II, *Weapon System Safety Guidelines Handbook System Safety Engineering and Management*.

Software System Safety Hazard Analysis

Step 1 – Perform a software Functional Hazard Analysis (FHA)

Software System Safety Hazard Analysis

Step 1 – Perform a software Functional Hazard Analysis (FHA)

Step 2 – For each SSSF, perform (and document) all required tasks.

For each analysis task, identify:

a. Potential Causal Factors

b. Potential (or actual) Mitigations

c. Appropriate In-Depth Safety-Specific Testing for each CF and Mitigation

FHA for Software

[the beginning of a MIL-STD-882E software safety effort]

Performing the Software FHA

Step 1 – Perform a software Functional Hazard Analysis (FHA)

a. Identify each Safety-Significant Function (SSF) that has been allocated to software (a SSSF).

b. Assess the level of software control of the function (the Software Control Category, or SCC).

c. Identify associated safety requirements or design constraints.

d. For highly critical (SwCI 1) SSSFs, identify potential system or software design redundancies to lower the SwCI (and required LoR).

MIL-STD-882E Guidance for FHA

[from Task 208 – Functional Hazard Analysis]

208.1 Purpose . . . The initial FHA should be accomplished as early as possible in the Systems Engineering (SE) process to enable the engineer to . . .

- identify and document SCFs, SCIs, SRFs, and SRIs;
- allocate and partition SCFs and SRFs in the software design architecture;
- and identify requirements and constraints to the design team.

A working definition for ‘Function’

The following is a working definition we will use for the term ”software function” (somewhat modeled after a mathematical function):

Given an input, or a set of related inputs, a software function produces one or more of the following outcomes:

- An externally observable system action;
- Externally observable digital information that can be used by a system operator or another software entity; or
- An internal change of digital state.

NOTE: The use of ‘external’ and ‘internal’ refers to the context of the software component(s).

Naming a Function

Name each SSSF using a verb (performing an action) and a noun (object of the verb):

Examples:

- Arm the warhead
- Detonate the warhead
- Arm the booster
- Ignite the booster
- Release the missile
- Safe the booster
- Fire the weapon

Choosing the 'size' of a SSSF

Use engineering judgement to choose the best 'size' of SSSFs for effective and efficient analysis and test - too high a level puts too much functionality all in the same "analysis bucket," while too low a level breaks the analysis into too many pieces.

Some examples:

- Too high: Perform a Standard Missile engagement
- Too low: Close the K1 relay
- Good level: Arm the missile booster

Functional Failure Types

[from NAVSEA SW020-AH-SAF-0010]

Function:

1 Fails to operate

2 Operates incorrectly/erroneously

3 Operates inadvertently

4 Operates at wrong time (early)

5 Operates at wrong time (late)

6 Unable to stop operation

7 Receives erroneous data

8 Sends erroneous data

9 Conflicting data or information

Performing the Software FHA

-- Step 1a --

Step 1a. Identify each Safety-Significant Function (SSF) that has been allocated to software (a SSSF).

- Use the nine functional failure types to reason about the different ways the SSSF might fail with potential safety impact.

  Ex. – Software-allocated missile release function fails to operate after missile ignition.

- Document the level of mishap severity that might result from the functional failure.

  Note: For the weapon systems and combat systems we work with, this is most often CAT for software functional failures.

Performing the Software FHA

-- Step 1b --

Step 1b. Assess the level of software control of the function (the Software Control Category, or SCC).

To claim Semi-autonomous SCC, document how each SSSF failure is detected and what the independent safety mechanism that mitigates or controls the resulting hazard is.

To claim Redundant Fault Tolerant SCC, document what the redundancies are and how they mitigate or control each safety-significant failure type for the SSSF.

Examples of SSSF Functional Failures

- Safe weapon SSSF fails to operate
- Arm warhead SSSF operates inadvertently
- Detonate warhead SSSF operates inadvertently
- Detonate warhead SSSF operates at wrong time (early)
- Detonate warhead SSSF operates at wrong time (late)

NOTE: The SSSF hazard severity or the software control category may vary for each functional failure type.

Performing the Software FHA

-- Step 1c --

Step 1c. Identify associated safety requirements or design constraints.

The safety requirements and design constraints are mitigations for the safety-significant SSSF failures. Communicate these with the system and software engineers to ensure:

- They are included in the requirements and design (or coding standards) for the system
- There are appropriate tests (or inspections or analyses) included to validate the mitigations work to control identified safety-significant failures for the SSSF.

Examples of Safety Requirements and Design Constraints

- The Launcher shall include an independent Canister Deluge sub-system to command Canister Flooding in case of Launcher Overtemperature or Missile Restrained Firing.
- The Launcher shall only process Missile Launch-related commands if the Launcher has been placed in Tactical Mode by the Weapon Control System.
- The Launcher shall allow the selection of no more than two Missiles for Launch at the same time.

Performing the Software FHA

-- Step 1d --

Step 1d. For highly critical, SwCI 1 SSSFs, identify potential system or software design redundancies that could lower the SwCI (and required LoR).

These fault tolerant redundancies are mitigations for safety-significant SSSF failures. Communicate these with the system and software engineers to ensure:

- They are included in the requirements and design for the system

Ex. – The Boeing 777 primary flight software is implemented in three similar computation channels (triple modular redundancy), each with three dis-similar ‘computation lanes’ (written in different programming languages).

FHA Advantages
[from NAVSEA SW020-AH-SAF-010 Section III]

The following are significant advantages of the [FHA]:

a. Is easily and quickly performed.
b. Does not require considerable expertise.
c. Is relatively inexpensive, yet provides meaningful results.
d. Provides rigor for focusing on hazards associated with system functions.
e. Good tool for software safety analysis.

FHA Disadvantages
[from NAVSEA SW020-AH-SAF-010 Section III]

The following are disadvantages of the [FHA]:

a. . . . it might overlook other types of hazards, such as those dealing with hazardous energy sources or sneak circuit paths.

b. After a functional hazard is identified, further analysis is required to determine if the causal factors are possible.

c. Cannot completely replace the need for a PHA.

In-Depth Safety-Specific Testing

In-Depth Safety-Specific Testing

1. In-Depth Safety-Specific Testing should be derived from the software safety analyses

In-Depth Safety-Specific Testing

1. In-Depth Safety-Specific Testing should be derived from the software safety analyses

2. Test cases should be assigned to appropriate test events

Booz | Allen | Hamilton

In-Depth Safety-Specific Testing

1. In-Depth Safety-Specific Testing should be derived from the software safety analyses

2. Test cases should be assigned to appropriate test events

3. Ensure results are captured for safety evidence

Limits of Testing

[W]e can thoroughly test hardware and get out requirements and design errors [but we c]an only test a small part of potential software behavior.

•Leveson, Nancy G., "A New Approach to Ensuring Safety in Software and Human Intensive Systems." SECIE Safety in Software and Human Intensive Systems. July 2009.

Complacency may also have been involved, i.e., the common assumption that software does not fail and that software testing is exhaustive and therefore additional software checking was not needed.

•Leveson, Nancy G., "A Systems-Theoretic Approach to Safety in Software-Intensive Systems." 2004.

Limits of Testing

[O]ne of the most important limitations of software testing is that testing can show only the presence of failures, not their absence. This is a fundamental, theoretical limitation; generally speaking, the problem of finding all failures in a program is undecidable.

•Paul Ammonn, Jeff Offutt. *Introduction to Software Testing*. 2008.

Limits of Testing

We cannot test software for correctness: Because of the large number of states (and the lack of regularity in its structure), the number of states that would have to be tested to assure that software is correct is preposterous. Testing can show the presence of bugs, but, except for toy problems, it is not practical to use testing to show that software is free of design errors.

•David L. Parnas, A. John van Schouwen, and Shu PO Kwan. "Evaluation of Safety-Critical Software." *Communications of the ACM*, June 1990.

An interview with Watts Humphrey

(the “Father of Software Quality”)

Humphrey: . . . When you think about a big program, big complex system program, 2 million lines of code something like that, and you run exhaustive tests, what percentage of all the possibilities do you think you’ve tested? Any idea?

Booch: Oh it’s going to be an embarrassingly small number probably in the less than 20, 30% would be my guess. . .

Humphrey: You’re way off. Way off. I typically ask people and I get back numbers 50%, 30%, that kind of thing. I asked the people at Microsoft, the Windows people, what they thought. And then we chatted about it a bit and they said about 1%.

Booch: Oh my goodness.

Humphrey: And my reaction is they’re high by several orders of magnitude. . . the number of possibilities is so extraordinary you literally couldn’t do a comprehensive test in the lifetime of the universe today.

“An Interview with Watts Humphrey, Part 26: Catastrophic Software Failures and the Limits of Testing” Watts S. Humphrey and Grady Booch, Aug 16, 2010, provided by the Computer History Museum.

Purpose of Testing

Assess quality. This is a tricky objective because quality is multi-dimensional. . . For example, reliability is . . . about the number of reliability-related failures that can be expected in a period of time or a period of use. . .To make this prediction, you need a mathematically and empirically sound model that links test results to reliability. Testing involves gathering the data needed by the model. . .

Verify correctness of the product. It is impossible to do this by testing.

Assure quality. Despite the common title, quality assurance, you can't assure quality by testing. . .

Assess conformance to specification. . .

Find defects. . . the classic objective of testing. . . Generally, we look for defects in all interesting parts of the product. . .

Kaner, C. "What Is a Good Test Case?" 2003.

Purpose of Safety-Specific Testing

In-Depth Safety-Specific Testing should clearly demonstrate additional testing rigor.

Test cases should attempt to show that:

1) Causal Factor instances ***can be realized*** and

2) Identified Mitigations ***don't work as intended***

The test scenarios should include credible "load" or "stress" relevant to the SSSF.

Types of In-Depth Testing

Boundary limit testing:

- Data range limits (e.g., highest or lowest possible values of a safety-critical input, at or near zero, or near/at/over capacity limits of a data storage).
- Timing limits (e.g., at the expiration of a timer or time limit).

Robustness testing:

- Response to abnormal inputs and conditions while ensuring safe SSSF performance, e.g., high rates of new track acquisitions and drop-outs.

Fault injection testing:

- Response to faults injected during SSSF performance.

Stress testing:

- Response to credible system stress during SSSF performance.

Types of In-Depth Testing

Safe state transition testing:

- Exercise all possible state transitions during SSSF performance.

Out of sequence testing:

- Software response to out-of-sequence inputs and conditions while ensuring safe performance of the SSSF.

Out-of-range value testing:

- Assurance of safe performance of the SSSF in response to out-of-range inputs or data values.

Error and exception handling testing:

- Response to errors and exceptions during SSSF performance.

Types of In-Depth Testing

Timing analysis testing:

- For safety-critical hard real time requirements, use targeted load or stress testing of the time-critical SSSF functionality to support the findings of timing analyses performed.

Algorithm correctness testing:

- Targeted stress testing of safety-critical algorithms associated with the SSSF.

Independent test:

- Testing of prioritized SSSFs by an independent test team, if determined to be needed by analysis.

Regression testing:

- Focused regression testing of SwCI 1 or 2 SSSF as determined from changes to related functionality.

Examples of In-Depth Testing

- Script a “Restrained Firing” in a Launcher followed immediately by a communication failure and “hand-off” of the Launcher to the alternate Launch Controller:
  - See if all missile launches in the Launcher are “safed,” as required after a Restrained Firing
- Script a second Launch Inhibit Command just as the first Launch Inhibit Command timeout is occurring, which should clear the first Launch Inhibit condition
- Script a “failover” of the primary Launch Controller to the alternate Launch Controller just after a Launch Inhibit Command has been processed.
- Script a “Restrained Firing” during a Max Launch test scenario.

Requirements Analysis

Safety Requirements Analysis (SRA)

The safety requirements are the driving force behind a designer's ability to design safety into a system and its subsystems. . .

From a safety perspective, there are three categories of SSRs [software safety requirements] . . . contributing software safety requirements (CSSR), generic software safety requirements [GSSR], and mitigating software safety requirements (MSSR).

[from the *Joint Software System Safety Engineering Handbook* (2010)]

Generic Software Safety Requirements (GSSRs)

GSSRs are requirements that have been documented over the years under the heading of lessons learned and best practices. . . The requirements themselves are not safety specific and may not yet be tied to a specific system hazard.

[from the *Joint Software System Safety Engineering Handbook* (2010)]

Some Example GSSRs

- The Launcher software shall adhere to all MISRA C++ guidelines for safety-critical software, with the exception of those documented, with rationale for non-compliance, in Table X.
- The Launcher software shall not perform dynamic memory allocation, except during program Initialization.
- The Launcher software shall not use C++ templates for any safety-significant software data objects or functions.

Contributing Software Safety Requirements (CSSRs)

The CSSRs are requirements that should already exist in the specifications and were likely authored by someone other than a safety engineer. CSSRs are related to the performance of the system to accomplish its intended function or mission. These requirements are not present for the mitigation or control of a hazard; in fact, they will often contribute to the existence of a hazard. An example of a CSSR is "Fire the Weapon." . . .

[from the *Joint Software System Safety Engineering Handbook* (2010)]

Some Example CSSRs

- The Launcher shall power up the Missile for preparation to launch on the receipt of a valid Missile Select Command.
- The Launcher shall arm the Missile's First Stage Booster on successful completion of Launch Preparation.
- The Launcher shall apply Ignition Power on detection of all Missile-Launcher Ready to Launch conditions.
- The Missile shall arm the Warhead on detection of Safe Separation from the Launch Platform.

Mitigating Software Safety Requirements (MSSRs)

MSSRs are requirements derived from in-depth mishap and hazard causal analyses. . . . the safety engineer [performs] the safety analysis to determine whether the GSSRs have successfully mitigated the known causal factors of the mishaps and hazards. . .

MSSRs are usually authored by safety engineers, with input and assistance from the design engineers and domain experts associated with the design or subsystem being analyzed. These MSSRs must be added to the specifications . . .

[from *Joint Software System Safety Engineering Handbook* (2010)]

Some Example MSSRs

- The Launcher Deluge subsystem shall continuously monitor for Canister and Launcher Overtemperature and for Restrained Firing, and command Canister Deluge on those Canisters effected by the occurrence of any detected Hazards.
- The Launcher shall set a 75 second timer for the completion of each Missile Launch Sequence, and Safe any selected Missile that has not completed a Launch within that time period.

Analysis of Requirements

Assess all tagged CSSRs/MSSRs for:

- Completeness
- Potential conflict with other requirements
- Ambiguity

Example Conflicting/Ambiguous

- Potential conflicting requirements:
  - Automated train doors must open only when train is stopped and properly aligned with the platform.
  - Automated train doors must open for evacuation in the event of an emergency.

- Potential ambiguous requirement:
  - Aircraft shall inhibit thrust reversal when the aircraft is in flight.

Architecture Analysis

Some Terminology
(from the JSSSEH and other sources)

Architecture: The organizational structure of a system or component (IEEE 610.12 – 1990).

- ‘Architecture is concerned with the selection of architectural elements, their interaction, and the constraints on those elements and their interactions’ (Perry & Wolf, 1992, p. 40-52).
- ‘Architecture focuses on the externally visible properties of software “components” (Bass, Clements, & Kazman, 1998).

System Architecture: The arrangement of elements and subsystems and the allocation of functions to meet system requirements (*INCOSE Systems Engineering Handbook*).

Safety in a Control System

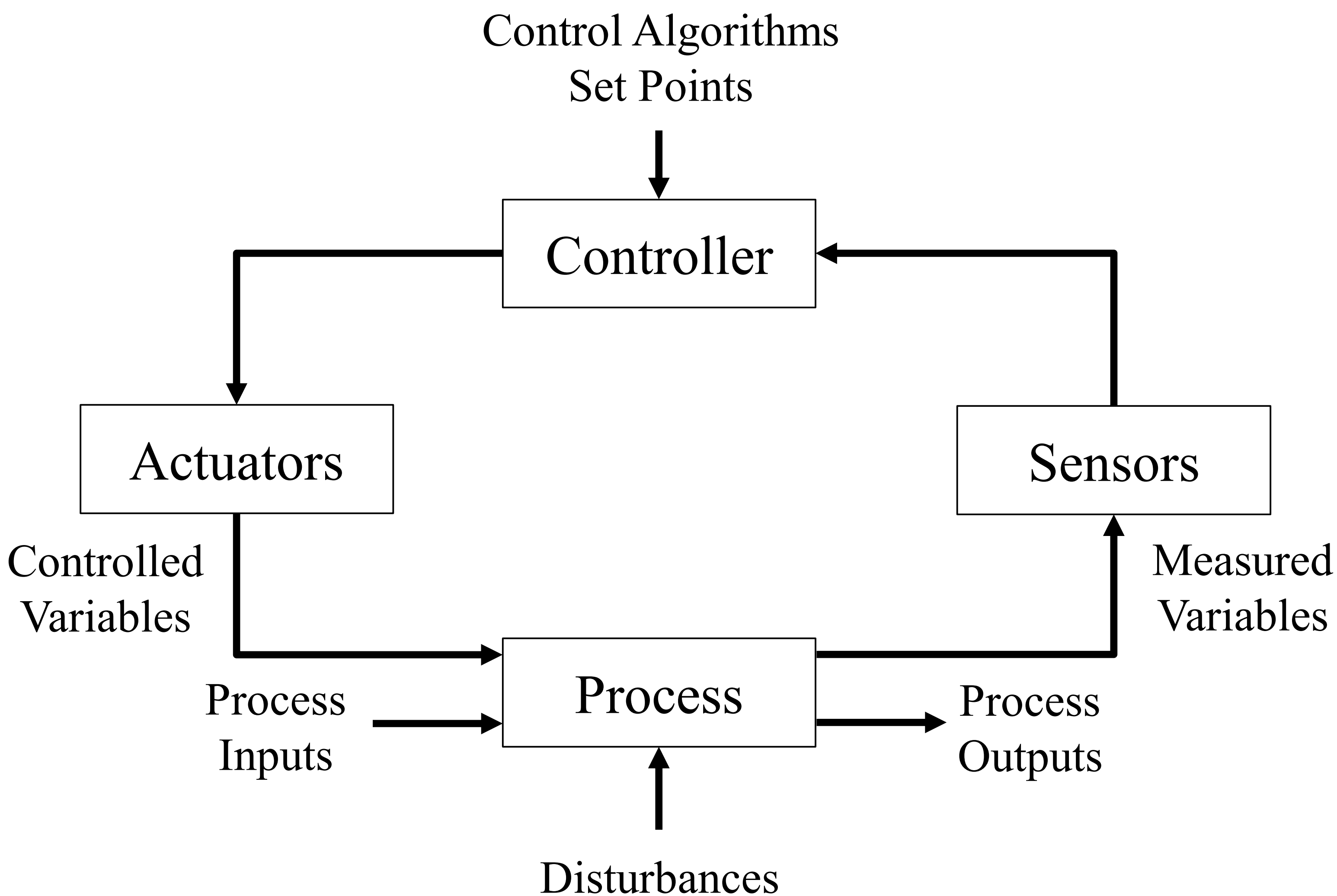
In control theory, open systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control.

. . . [A]ccidents often occur . . . as a result:

1. Incorrect or unsafe control commands are given
2. Required control actions (for safety) are not provided
3. Potentially correct control commands are provided at the wrong time (too early or too late), or
4. Control is stopped too soon or applied too long.

Nancy G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*, 2011.

The Classic "Control Loop"



Inter-Process Architecture Analysis

- Treat each distributed SSSF as a control loop allocated across the system architecture.
- Think of ways the control or feedback signals (messages) might be corrupted, delayed or lost (potential Causal Factors).
- For each of the Causal Factors identified, think of existing or potential mitigations.

System Path/Thread Analysis for a 'Safe Weapon' SSSF

Operator		CSCI 1		CSCI 2
[]	Safe Wpn →	[]		[]
[]		[]	Safe Wpn →	[]
[]		[]	←Ack/Nak	[]
[]	←WILCO (or	[]		[]
[]	CANTPRO)	[]		[]

CSCI = Computer Software Configuration Item
WILCO = "Will Comply"
CANTPRO = "Cannot Process"

Ack = 'Valid' Message Acknowledge
Nak = 'Invalid' Message (Negative) Acknowledge
Safe Wpn = Safe Weapon

More Robust ‘Architecture’ for a ‘Safe Weapon’ SSSF

Operator		CSCI 1		CSCI 2
[]	Safe Wpn →	[]		[]
[]	←Ack/Nak	[]		[]
[]		[]	Safe Wpn* →	[]
[]		[]	←Ack/Nak	[]
[]		[]	←HAVCO**	[]
[]	←HAVCO**	[]		[]
[]		[]		[]

* CSCI 1 timer on CSCI 2’s HAVCO/CANTCO response

** or CANTCO

CSCI = Computer Software Configuration Item
HAVCO = “Have Complied”
CANTCO = “Cannot Comply”

Ack = ‘Valid’ Message Acknowledge
Nak = ‘Invalid’ Message (Negative) Acknowledge
Safe Wpn = Safe Weapon

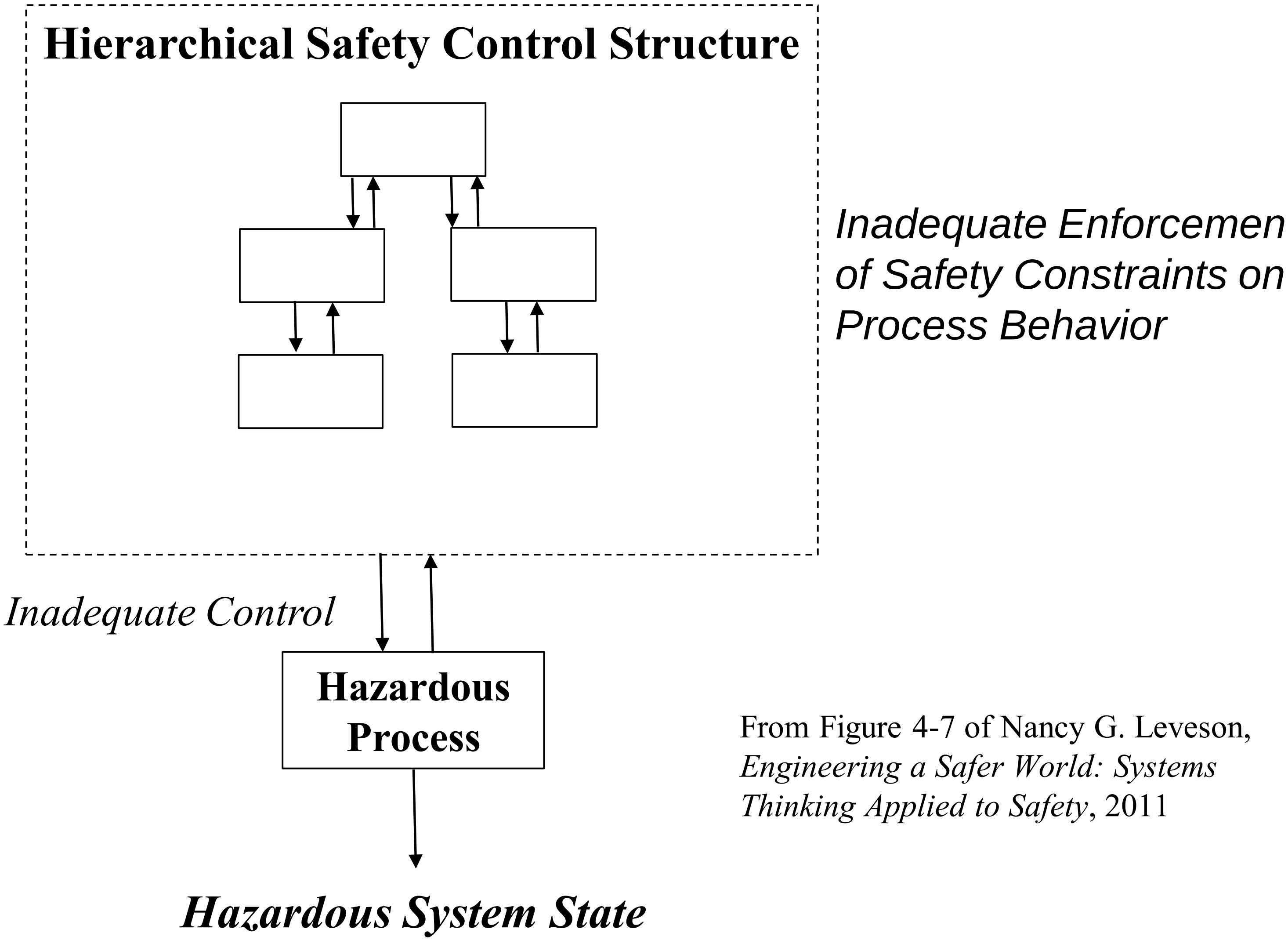
System-Theoretic Accident Model and Processes (STAMP)

In systems theory, emergent properties, such as safety, arise from the interactions among the system components. The emergent properties are controlled by imposing constraints on the behavior and the interactions among the components. Safety then becomes a control problem where the goal of the control is to enforce the system constraints. Accidents result from inadequate control or enforcement of safety-related constraints on the development, design, and operation of the system.

. . . Feedback is a basic part . . . of treating safety as a control problem. Information flow is a key in maintaining safety.

Nancy G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*, 2011.

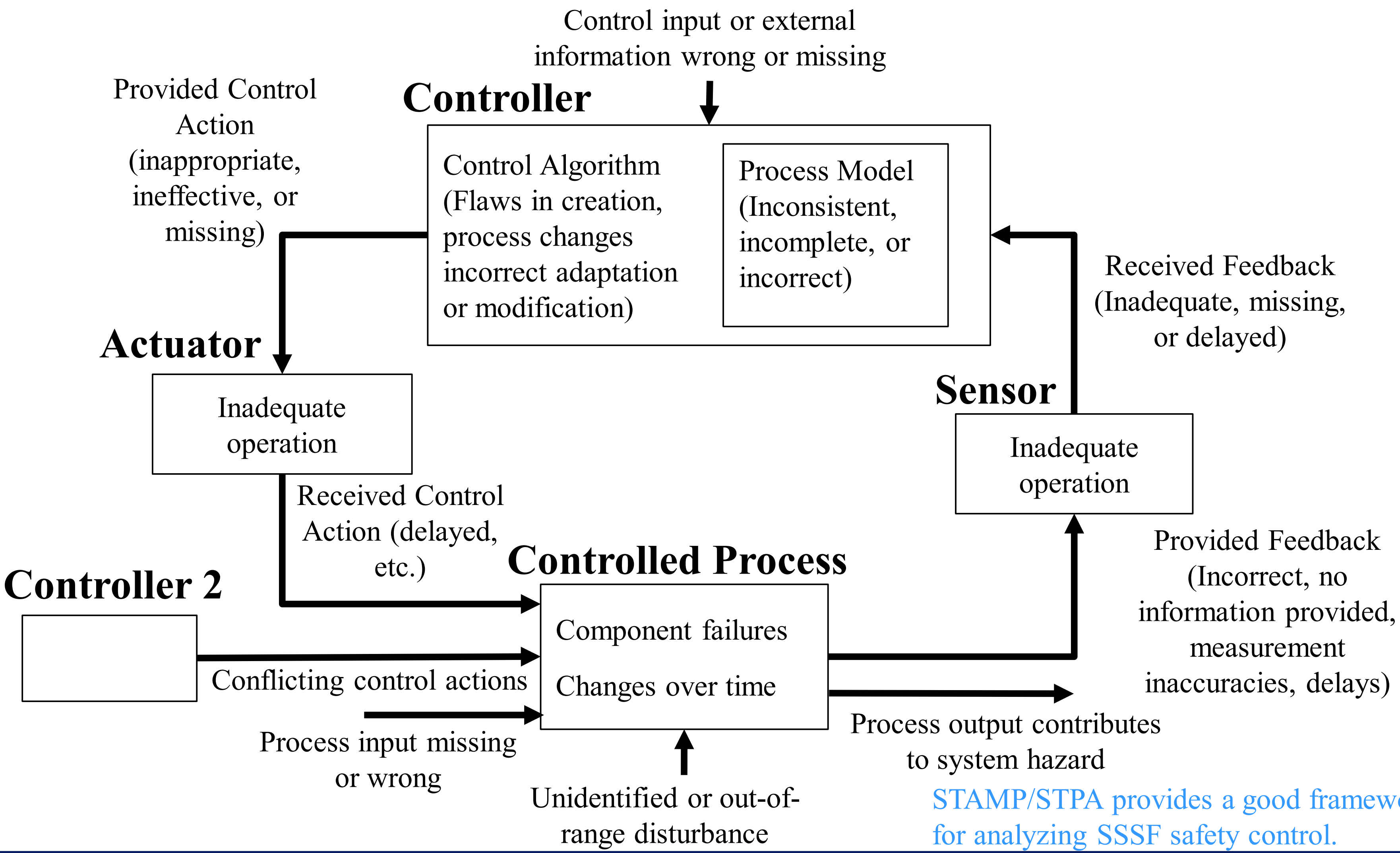
STAMP View of System Safety



From Figure 4-7 of Nancy G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*, 2011

General Control Loop with Causal Factors

(from *Safety Assurance in NextGen*, NASA/CR-2012-217553)



STAMP/STPA provides a good framework for analyzing SSSF safety control.

Some Thoughts On STAMP, STPA, and Meeting MIL-STD-882E Required LoR

We do not assign a SwCI because in STAMP software can and should be treated in the same way as hardware, i.e., the hazards are identified along with causal scenarios leading to the hazards. Then engineers can eliminate or mitigate those causes according to standard system safety practice and design precedence . . .

> Nancy G. Leveson, “STPA (System-Theoretic Process Analysis) Compliance with Army Safety Standards and Comparison with SAE ARP 4761,” a whitepaper on the compliance of STPA with MIL-STD-882E and Army AMCOM Regulation 385-17.

Some Thoughts On STAMP, STPA, and Meeting MIL-STD-882E Required LoR

We do not assign a SwCI because in STAMP software can and should be treated in the same way as hardware, i.e., the hazards are identified along with causal scenarios leading to the hazards. Then engineers can eliminate or mitigate those causes according to standard system safety practice and design precedence . . .

Nancy G. Leveson, “STPA (System-Theoretic Process Analysis) Compliance with Army Safety Standards and Comparison with SAE ARP 4761,” a whitepaper on the compliance of STPA with MIL-STD-882E and Army AMCOM Regulation 385-17.

THOUGHTS:

- STAMP/STPA is a very good framework for software safety architecture analysis.

Some Thoughts On STAMP, STPA, and Meeting MIL-STD-882E Required LoR

We do not assign a SwCI because in STAMP software can and should be treated in the same way as hardware, i.e., the hazards are identified along with causal scenarios leading to the hazards. Then engineers can eliminate or mitigate those causes according to standard system safety practice and design precedence . . .

Nancy G. Leveson, “STPA (System-Theoretic Process Analysis) Compliance with Army Safety Standards and Comparison with SAE ARP 4761,” a whitepaper on the compliance of STPA with MIL-STD-882E and Army AMCOM Regulation 385-17.

THOUGHTS:

- STAMP/STPA is a very good framework for software safety architecture analysis.
- It would be a very “heavy lift” for an individual program or PFS to make the case that STAMP/STPA is replacement for required LoR.

Some Thoughts On STAMP, STPA, and Meeting MIL-STD-882E Required LoR

We do not assign a SwCI because in STAMP software can and should be treated in the same way as hardware, i.e., the hazards are identified along with causal scenarios leading to the hazards. Then engineers can eliminate or mitigate those causes according to standard system safety practice and design precedence . . .

Nancy G. Leveson, “STPA (System-Theoretic Process Analysis) Compliance with Army Safety Standards and Comparison with SAE ARP 4761,” a whitepaper on the compliance of STPA with MIL-STD-882E and Army AMCOM Regulation 385-17.

THOUGHTS:

- STAMP/STPA is a very good framework for software safety architecture analysis.
- It would be a very “heavy lift” for an individual program or PFS to make the case that STAMP/STPA is replacement for required LoR.
- My experience has been that MANY software problems are not at the architecture level (and can’t be eliminated there).

Design Analysis

What is “Design”?

‘Design focuses on the properties of software “components” that are not externally visible.’

[S. Whitford, 2015]

Design

What is NOT Externally Visible

What is NOT externally visible?

- The organization of elements inside each software component, e.g.:
  - Is it object oriented (Java, C++) or not (C, Assembler)?
  - Is it single threaded or multi-threaded?
- The data flow between the elements inside each software component, e.g.:
  - Message passing
  - Call parameters
  - Global data
- The control flow between the elements inside each software component, e.g:
  - Procedure/function calls
  - Semaphores/mutexes/monitors

Safety-Critical Decision Points

- Most SwCI 1 or SwCI 2 SSSFs are safety-critical because the software has command authority over a safety-critical system action.

Safety-Critical Decision Points

- Most SwCI 1 or SwCI 2 SSSFs are safety-critical because the software has command authority over a safety-critical system action.
- The software is therefore responsible for making the decision to take that action, often the release of lethal energy.

Safety-Critical Decision Points

- Most SwCI 1 or SwCI 2 SSSFs are safety-critical because the software has command authority over a safety-critical system action.
- The software is therefore responsible for making the decision to take that action, often the release of lethal energy.
- If the data used to make the safety-critical decision is corrupted or stale, the software can make the wrong decision with catastrophic results.

Safety-Critical Decision Points

- Most SwCI 1 or SwCI 2 SSSFs are safety-critical because the software has command authority over a safety-critical system action.
- The software is therefore responsible for making the decision to take that action, often the release of lethal energy.
- If the data used to make the safety-critical decision is corrupted or stale, the software can make the wrong decision with catastrophic results.
- Design (and Code) Analysis should be focused on how the software maintains, or could fail to maintain, the integrity of the data used at each Safety-Critical Decision Point in the SSSF.

SCDP: An Example

Is it safe to launch the missile?

- Was a valid Launch Command received from the Operator?
- Is the Cell Hatch fully open?
  - Does the Cell Hatch No. 1 sensor report “open”?
  - Does the Cell Hatch No. 2 sensor report “open”?
- Is the Uptake Hatch fully open?
  - Does the Uptake Hatch No. 1 sensor report “open”?
  - Does the Uptake Hatch No. 2 sensor report “open”?
- Has it been long enough since the last missile lunched?
- Is the Close-In Weapon System (CIWS) ***not*** currently firing? (Implemented as a launchInhibited Boolean (TRUE/FALSE) data item.)

‘Launch Inhibited’ implemented with multiple threads

Thread A:

[Launch Missile Command received]

```
boolean isMslLaunchOK ()
   If . . . hatch statuses and
             last missile launch time are “ok”
   . . . && (launchInhibited == FALSE)
        return TRUE
   else
        return FALSE
```

launchInhibited is set to TRUE when a CIWS engagement is about to start.

‘Launch Inhibited’ implemented with multiple threads (cont’d)

Thread B (higher priority):

[Launch Inhibit Command received]

. . .

setLaunchInhibit ()
. . . *if old timer active, cancel it*
. . . launchInhibited = TRUE
. . . *Initiate a 20s timer to clear inhibit*

Thread C (lower priority):

[20s Launch Inhibit timer expires]

. . .

clearLaunchInhibit ()
. . . launchInhibited = FALSE

Intent is to clear a *pre-existing* Launch Inhibit condition after 20 seconds.

Analysis of 'Launch Inhibited'

Thread B (higher priority):

[Receipt of new Launch Inhibit command unblocks thread]
. . .
setLaunchInhibit ()
. . . *if old timer active, cancel it (but, it's too late)*
. . . launchInhibited = TRUE
. . . *Initiate a (new) 20s timer*
[thread blocks on task completion]

Thread C (lower priority):

[Old 20s Launch Inhibit timer expires]
. . .

clearLaunchInhibit ()
. . . launchInhibited = FALSE

Timer intended to clear OLD Launch Inhibit condition clears NEW one instead!.
A data synchronization mechanism should be used to protect the shared data item.

Some Sources of Design Causal Factors

Establish the pros and cons of the design of each software component to which the SSSF is allocated and determine whether they could be Causal Factors or Mitigations for a SSSF functional failure due to an erroneous Safety-Critical Decision by the software. (It's all about the safety-critical data integrity.)

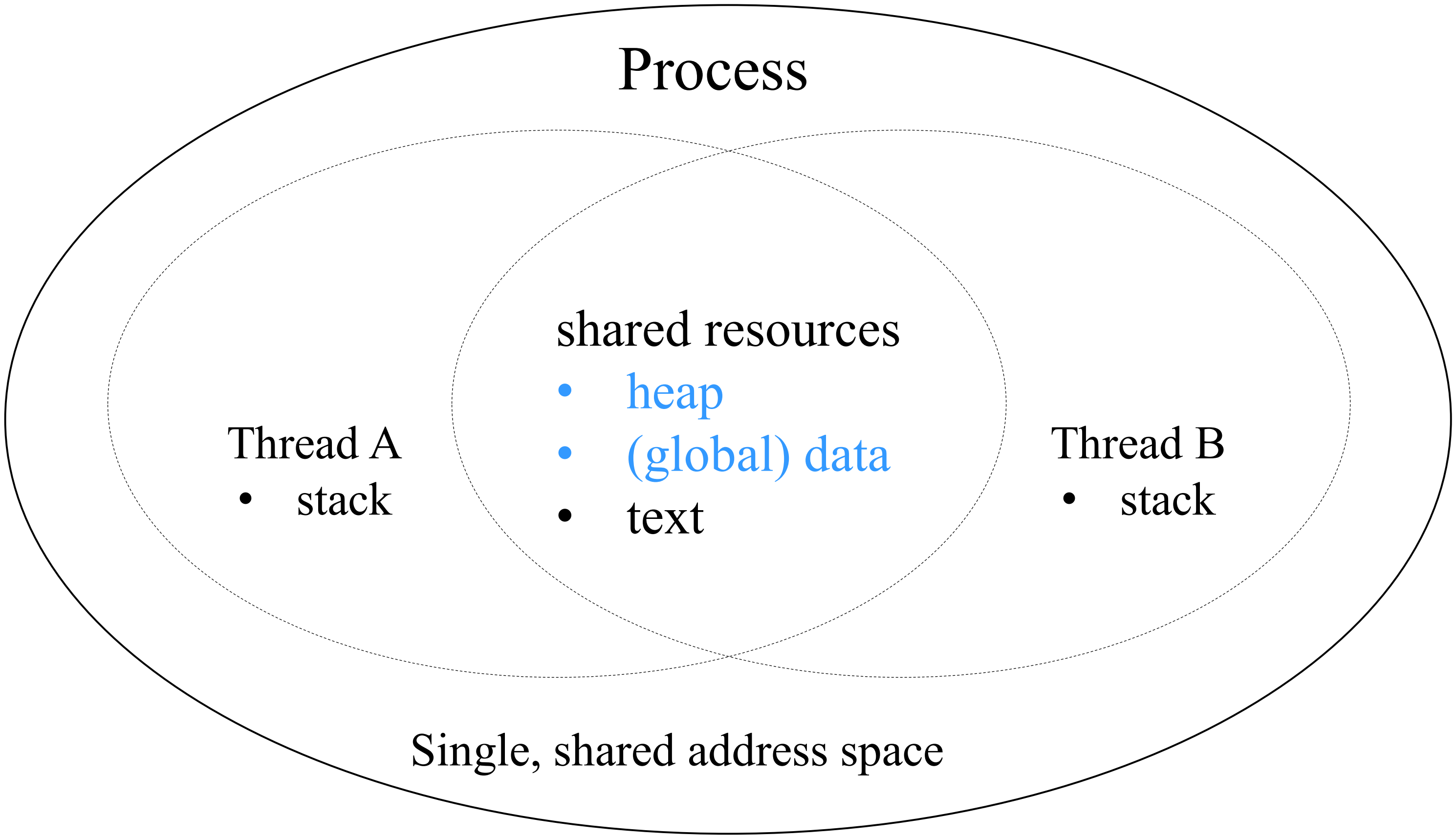
Some Sources of Design Causal Factors

Establish the pros and cons of the design of each software component to which the SSSF is allocated and determine whether they could be Causal Factors or Mitigations for a SSSF functional failure due to an erroneous Safety-Critical Decision by the software. (It's all about the safety-critical data integrity.)

Design weaknesses with respect to data integrity, e.g.:

- Shared data "race conditions"
- Loss of data in software "failovers"
- Failure to refresh temporal data
- Unhandled exceptions

Multi-(two)threaded Design



Variables or objects in the *heap* or *data* can be shared by the threads. This can lead to race conditions or thread deadlock. (*Text* can also be shared, but (usually) does not change in value.)

Pros and Cons of Multi-threaded Design

Pros for multi-threaded design:

- Allows software to be more responsive to an unpredictable external environment (new inputs from an operator, another computer, or a sensor)
- Each thread can be ‘appropriately prioritized’

Cons for single threaded design:

- Improperly synchronized threads can corrupt shared data
- Improperly synchronized threads can deadlock (block each other forever)
- Improperly prioritized threads can cause starvation or unpredictable delays
- Much more difficult to analyze or test than single-threaded designs

On the Difficulties with Multi-threading

'Concurrency in software is difficult. However, much of this difficulty is a consequence of the abstractions for concurrency that we have chosen to use. The dominant one in use today for general-purpose computing is threads. But non-trivial multi-threaded programs are incomprehensible to humans.'

[*The Problem with Threads,* Technical Report No. UCB/EECS-2006-1, Edward A. Lee, Professor, Chair of EE, Associate Chair of EECS, University of California at Berkley, January 10, 2006]

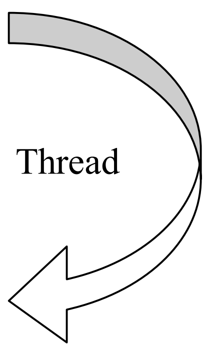
Single Threaded Design

A (usually infinite) loop, for an embedded program to "do its thing forever."

- Checks for input(s) [e.g., messages, sensor inputs]
- Performs any necessary processing of the input(s)
- Produces output(s) [e.g., messages, actuator control signals]

Example:

```
int main(void)
{   // initialization code here – done once
    for ( ; ; )  // or while (true) or while (1)
   { // read or detect stuff
     // do some calculation
     // write or command stuff
    }
 }
```



Pros and Cons of Single Threaded Design

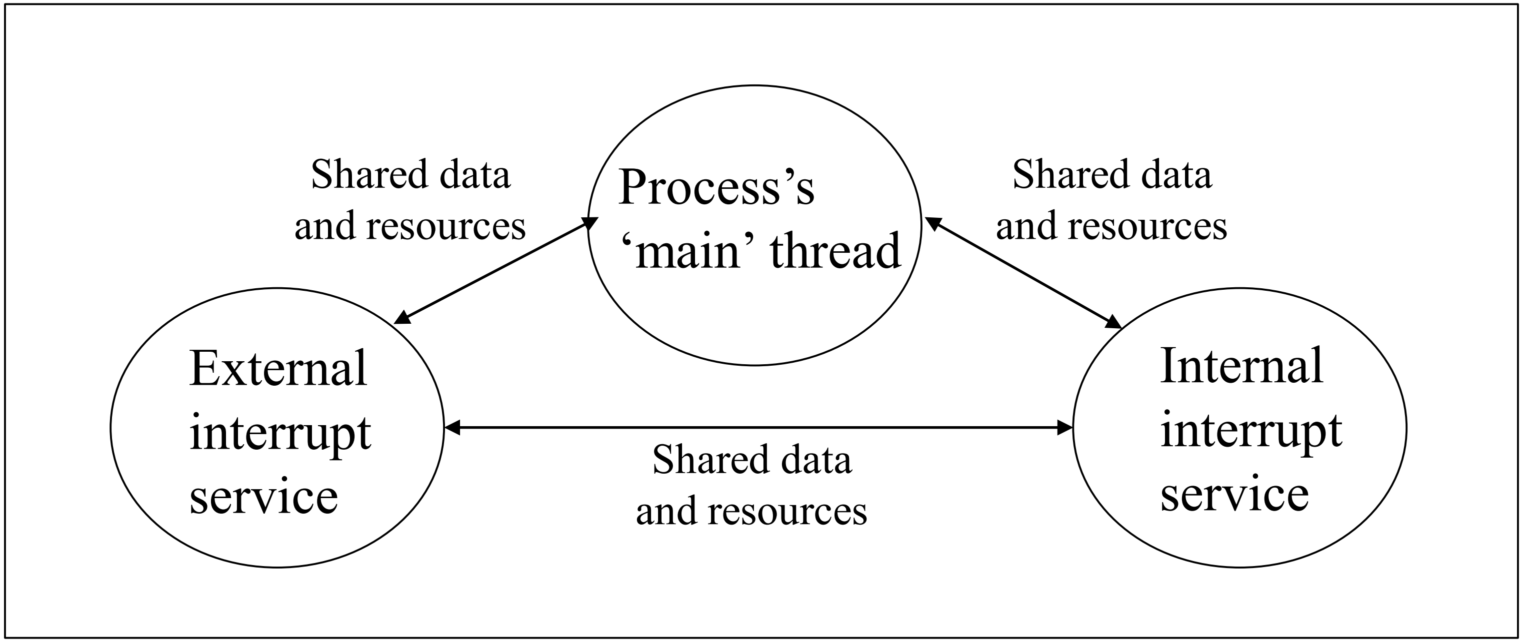
Pros for single threaded design:

- Easier to perform analysis (e.g., design, code, worst case timing)
- Easier to implement the first time

Cons for single threaded design:

- Delay in responding to external inputs
- Can become a bottleneck in the larger system
- Hard to prioritize multiple competing “tasks”
- Must implement the details for handling all I/O
- Becomes hard to maintain as more functionality is added

Single Threaded Design With Interrupt Service



- With few exceptions, Interrupt Service Routines (ISRs) should be short and sweet. For input, read the data into a buffer or queue, set a flag for 'main' to see, then get out of the way (let 'main' process the data).
- Non-atomic access by 'main' to data shared with an ISR must be protected from potential corruption (e.g., locking out the interrupt that drives the ISR while 'main' is reading from or writing to the shared data).

Pros and Cons of Design With Interrupt Service

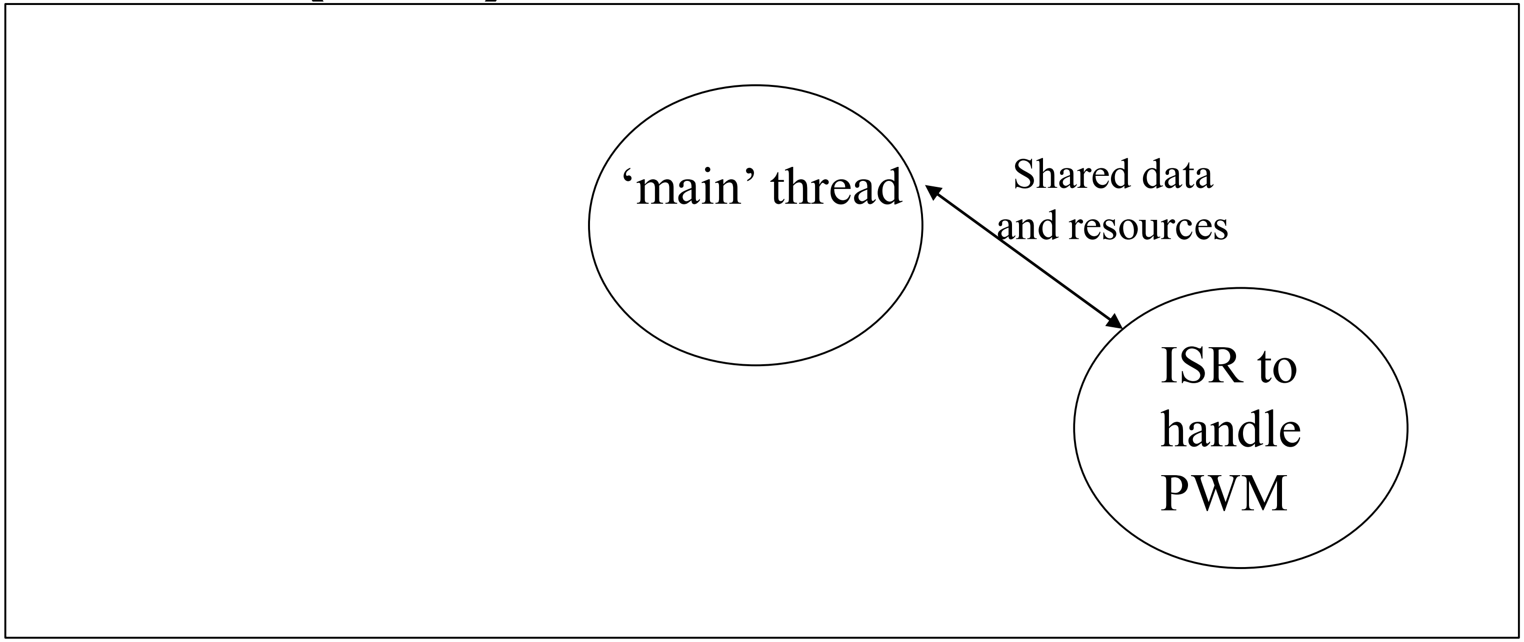
Pros for single threaded design with interrupt service:

- Somewhat more responsive to external inputs
- Relatively easy to perform analysis (e.g., design, code, worst case timing)
- Still easy to implement the first time

Cons for single threaded design with interrupt service:

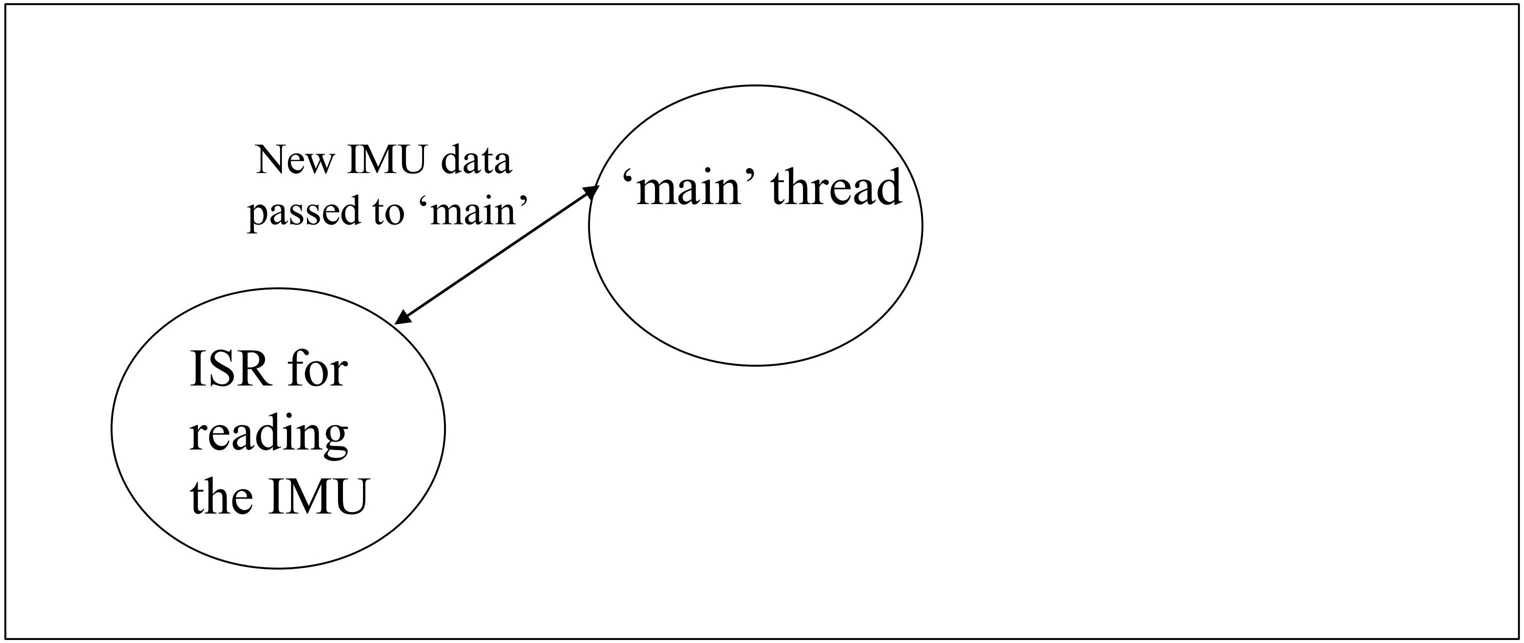
- Delay in responding to external inputs
- Main loop can still become a bottleneck (input queue overflow, delay in responding to external system)
- Still hard to prioritize multiple competing “tasks”
- Potential for corrupting data shared between ISRs and ‘main’
- Still hard to maintain as more functionality is added

Details of Pulse Width Modulation (Mis-)handled in the ISR



- A Programmable Power Supply was implemented so that almost all processing of sensors and control commands for pulse-width modulation (PWM) of the power output to power up missiles in a launcher for preparation to launch was performed inside the ISR.
- When a new missile was introduced, the interrupt occurred every 10 u-sec's and the ISR to 11 u-sec's to execute the additional processing for the power requirements for the new missile's launch preparation.

An ISR / 'main' example of non-atomic data sharing



- Non-atomic access by 'main' to data shared with an ISR must be protected from potential corruption (e.g., locking out the interrupt that drives the ISR while 'main' is reading from or writing to the shared data).
- Inertial Measurements include several values - linear accelerations (x, y, and z) and rotational measurements (about each axis). Is the IMU ISR locked out while 'main' is reading the shared IMU data?

Code Analysis

Code Analysis vs. Design Analysis

The difficulty of using the term "design" in relation to software is that in some sense, the source code of a program is the design for the program that it produces.

[*Wikipedia* article on “Software Design,” February 7, 2015]

Focus for LoR 1 Code Analysis

SwCI 1 code is typically responsible for releasing potentially catastrophic energy or for detecting a potentially catastrophic hazardous condition. Either way that usually involves one or more Safety-Critical Decision Points (SCDPs) in the software. These SCDPs use one or more software data items to make the decision.

- Focus code analysis on identification of internal data items used by software to make critical decisions to perform a safety-critical action or not.
    - Scope may expand as analysis progresses.
- Investigate how a data item's value is set and referenced by the software.
- Static or dynamic code analysis tools should be used for a detailed analysis and to document important technical aspects.

Program Slicing

In computer programming, program slicing is the computation of the set of programs statements, the program slice, that may affect the values at some point of interest, referred to as a slicing criterion. Program slicing can be used in debugging to locate source of errors more easily. Other applications of slicing include software maintenance, optimization, program analysis, and information flow control.

[*Wikipedia* article on "Program Slicing," March 17, 2015]

Some Code Analysis Tools

Tools to help an analyst explore the code:

- Eclipse (Java, C/C++) (Open Source Software)
- NetBeans (Java, C++)
- Understand for C++/Java (SCI Tools)

Tools to do automated static code analysis:

- CodeSonar (GrammaTech)
- Klocwork (Rogue Wave)
- Code Advisor (Coverity)
- PC-lint (Gimpel Software)

Code Analysis

1. For each SwCI 1 SSSF, identify and locate the SCDPs associated the SSSF.
2. Using appropriate automated or semi-automated code analysis tools, perform a “backward flow” analysis of the code from safety-critical decision points in the software.
3. Based on the results of the Requirements, Architecture, and Design Analyses, perform other appropriate code analyses, especially analysis of the implementation of safety critical mitigations for the SSSF.

Code Analysis

-- Step 1 --

1. For each SwCI 1 SSSF, identify and locate the SCDPs associated the SSSF.

- Locate the code that performs energy release. e.g., weapon firing, detonation, booster ignition. (potential Causal Factor) or that detects and responds to a hazardous condition.

An Example L-DETS SCDP

Source code for safety-critical function SetFirePulse and associated functions in file SafetyCritical_RX.c

```
//**********************************************************************
// @Function      void SetFirePulse(void)
//----------------------------------------------------------------------
// @Description   This function applies a 30 millisecond firing Pulse to detonate the unit.
//**********************************************************************
void SetFirePulse(void)
{
    if(G_SCV.SC_DisableSafetyCriticalProcessing == SC_PROCESSING_ENABLED)
    {
        if(IsArmPinRemoved() == ARM_PIN_HAS_BEEN_REMOVED)
        {                                   // When pin is pulled we get a high
                FIRE_PULSE_PORT = 1;
                G_SCV_PortFImage |= FIRE_PULSE_BIT;
                G_SCV.SC_DetonatorHasFired = DETONATOR_HAS_FIRED;
                DelayMilliSecondsNoInterrupt(30);
                SetToSafeState();
        }
    }
}
```

Is detonation currently enabled?

Code Analysis

-- Step 2 --

2. Using appropriate automated or semi-automated code analysis tools, perform a “backward flow” analysis of the code from safety-critical decision points in the software.

- The analysis should focus on identifying potential causes of stale or corrupt data being present at the safety-critical decision point.

An Example L-DETS SCDP (cont'd)

Control Flow Analysis: How is SetFirePulse called in the L-DETS Detonator software?

Callers of SetFirePulse() - /LDETS/src/SafetyCritical_RX.c - in workspace

- SetFirePulse() : void
  - DetonateUnit() : void
    - PerformCommand(const SC_Command_Message_u *) : int
      - ReceiveMessage() : int
        - ListenMode() : void
          - main() : int
    - ReceiveMessage() : int
      - ListenMode() : void
        - main() : int

SetFirePulse is only called from the function DetonateUnit, which is called on two paths within the "main" thread: one if the Fire Command is received directly from the Controller and the second if it has been forwarded from another Detonator.

An Example L-DETS SCDP (cont'd)

Data Flow Analysis: Where/how is SC_DisableSafetyCriticalProcessing updateded?

References to '(anonymous)::SC_DisableSafetyCriticalProcessing' (11 matches)

- LDETS
  - src
    - SafetyCritical_RX.c (11 matches)
      - ChargeCapacitor, line 82: if(G_SCV.SC_DisableSafetyCriticalProcessing == SC_PROCESSING_ENABLED)
      - EnableFiring, line 109: if(G_SCV.SC_DisableSafetyCriticalProcessing == SC_PROCESSING_ENABLED)
      - SetFirePulse, line 175: if(G_SCV.SC_DisableSafetyCriticalProcessing == SC_PROCESSING_ENABLED)
      - EnableSafetyCriticalProcessing, line 336: G_SCV.SC_DisableSafetyCriticalProcessing = SC_PROCESSING_ENABLED;
      - DisableSafetyCriticalProcessing, line 354: G_SCV.SC_DisableSafetyCriticalProcessing = SC_PROCESSING_DISABLED;
      - ClearSafetyCriticalVariables, line 377: G_SCV.SC_DisableSafetyCriticalProcessing = SC_PROCESSING_ENABLED;
      - ClearSafetyCriticalVariables, line 381: G_SCV.SC_DisableSafetyCriticalProcessing = SC_PROCESSING_DISABLED;
      - ClearSafetyCriticalVariables, line 401: if(G_SCV.SC_DisableSafetyCriticalProcessing != SC_PROCESSING_ENABLED)
      - ClearSafetyCriticalVariables, line 416: if(G_SCV.SC_DisableSafetyCriticalProcessing != SC_PROCESSING_DISABLED)
      - PowerUpClearSafetyCriticalVariables, line 450: G_SCV.SC_DisableSafetyCriticalProcessing = SC_PROCESSING_DISABLED;
      - PowerUpClearSafetyCriticalVariables, line 468: if(G_SCV.SC_DisableSafetyCriticalProcessing != SC_PROCESSING_DISABLED)

SC_DisableSafetyCriticalProcessing is only enabled and disabled at five locations in the software. Understanding the purpose and use of each location is needed to assess for potential weaknesses or problems..

Blue highlighting indicates SC_DisableSafetyCriticalProcessing is referenced but not changed.

An Example L-DETS SCDP (cont'd)

Data Flow Analysis: Where/how is SC_DisableSafetyCriticalProcessing updateded?

References to '(anonymous)::SC_DisableSafetyCriticalProcessing' (11 matches)

- LDETS
  - src
    - SafetyCritical_RX.c (11 matches)
      - ChargeCapacitor, line 82: if(G_SCV.SC_DisableSafetyCriticalProcessing == SC_PROCESSING_ENABLED)
      - EnableFiring, line 109: if(G_SCV.SC_DisableSafetyCriticalProcessing == SC_PROCESSING_ENABLED)
      - SetFirePulse, line 175: if(G_SCV.SC_DisableSafetyCriticalProcessing == SC_PROCESSING_ENABLED)
      - EnableSafetyCriticalProcessing, line 336: G_SCV.SC_DisableSafetyCriticalProcessing = SC_PROCESSING_ENABLED;
      - DisableSafetyCriticalProcessing, line 354: G_SCV.SC_DisableSafetyCriticalProcessing = SC_PROCESSING_DISABLED;
      - ClearSafetyCriticalVariables, line 377: G_SCV.SC_DisableSafetyCriticalProcessing = SC_PROCESSING_ENABLED;
      - ClearSafetyCriticalVariables, line 381: G_SCV.SC_DisableSafetyCriticalProcessing = SC_PROCESSING_DISABLED;
      - ClearSafetyCriticalVariables, line 401: if(G_SCV.SC_DisableSafetyCriticalProcessing != SC_PROCESSING_ENABLED)
      - ClearSafetyCriticalVariables, line 416: if(G_SCV.SC_DisableSafetyCriticalProcessing != SC_PROCESSING_DISABLED)
      - PowerUpClearSafetyCriticalVariables, line 450: G_SCV.SC_DisableSafetyCriticalProcessing = SC_PROCESSING_DISABLED;
      - PowerUpClearSafetyCriticalVariables, line 468: if(G_SCV.SC_DisableSafetyCriticalProcessing != SC_PROCESSING_DISABLED)

SC_DisableSafetyCriticalProcessing is only enabled at two locations in the software.

Blue highlighting indicates SC_DisableSafetyCriticalProcessing is referenced but not changed.

Code Analysis
-- Step 3 --

3. Based on the results Requirements Analysis, Architecture Analysis, or Design Analysis, perform other appropriate code analyses that might have potential safety-critical impacts, such as:

- **Timing analysis** – for safety-critical hard real time requirements, using appropriate static or dynamic code analysis tools to analyze the worst case execution time (WCET).
- **Interrupt analysis** – analysis of the coordination of interrupt handling with interruptible and non-interruptible safety-critical processing.
- **Algorithm correctness** – analysis of the correctness of the implementation of any safety-critical algorithm(s)..
- **Data structure/usage analysis** – analysis of the structure and use of safety-critical data objects associated with the SSSF.
- **OS function analysis** - analysis of correct use of OS functions used to implement LOR 1 functionality for the SSSF.

Wrap Up

Some Key Points

- Purpose of LoR is to focus and manage

Some Key Points

- Purpose of LoR is to focus and manage
- Software FHA should:
  - Be performed as early as reasonable
  - “Rack and stack” SSSFs by SwCI/LoR
  - Identify potential redundancies to reduce SwCI 1 SSSFs

Some Key Points

- Purpose of LoR is to focus and manage

- Software FHA should:
  - Be performed as early as reasonable
  - "Rack and stack" SSSFs by SwCI/LoR
  - Identify potential redundancies to reduce SwCI 1 SSSFs

- Requirements analysis should focus on:
  - Incompleteness
  - Ambiguities
  - Conflicts

Some Key Points

- Architecture analysis should focus on weaknesses in the command and control of distributed Safety-Significant Software Functions

Some Key Points

- Architecture analysis should focus on weaknesses in the command and control of distributed Safety-Significant Software Functions

- Design and code analysis should focus on Safety-Critical Decision Points (can the internal data items used by the software be corrupted or stale)

Some Key Points

- Architecture analysis should focus on weaknesses in the command and control of distributed Safety-Significant Software Functions

- Design and code analysis should focus on Safety-Critical Decision Points (can the internal data items used by the software be corrupted or stale)

- In-Depth Safety-Specific Testing should be derived from the analysis results

Some Key Points

- Architecture analysis should focus on weaknesses in the command and control of distributed Safety-Significant Software Functions
- Design and code analysis should focus on Safety-Critical Decision Points (can the internal data items used by the software be corrupted or stale)
- In-Depth Safety-Specific Testing should be derived from the analysis results
- All analyses and testing should be focused on Causal Factors and Mitigations

Best Practices for the Architecture, Design, and Modernization of Defense Models and Simulations

Dr. Katherine L. Morse, JHU/APL

Brian Miller, US Army CERDEC NVESD

Michael Heaphy, OSD(AT&L)/DMSCO

Outline

- **Overview**
  - What the DMSRA is and isn't
  - Goals/Vision/Motivation
  - Composable simulation architecture
- **Challenges**
  - Architectural and engineering
  - Enterprise-wide interoperability and reuse
- **Best practices (patterns)**
  - Identified
  - Planned additions
- **Conclusions**

Overview

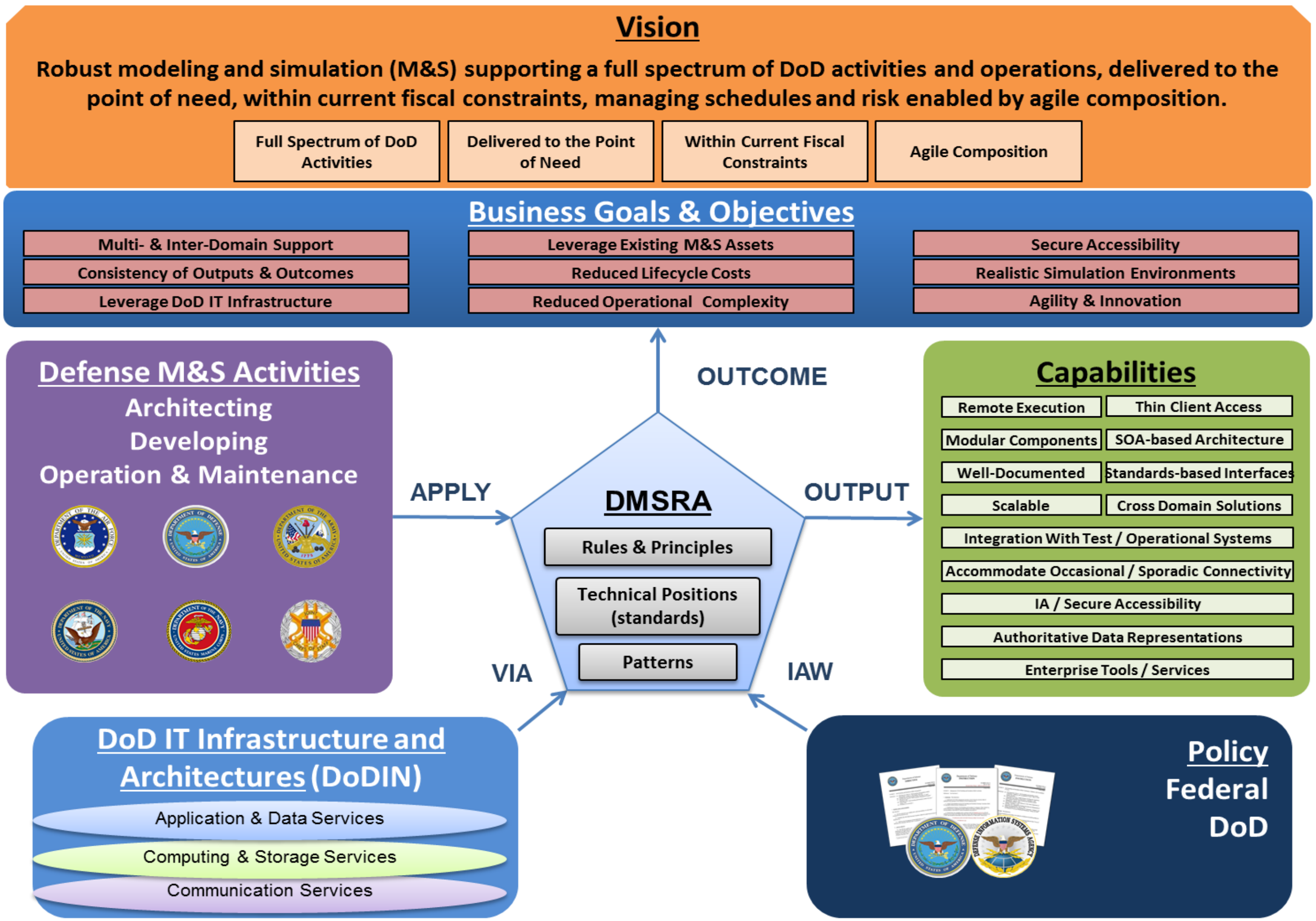
- **The DMSRA is NOT a solution architecture.**
- **It establishes a vision for Defense M&S:**
  – that leverages emerging technologies, and enterprise services;
  – to promote reuse and interoperability.
- **The DMSRA provides broadly applicable guidance.**
  – It captures principles, standards, and best practices for simulation architects and engineers to align on the vision.
  – It is not mandatory.

DMSRA Vision

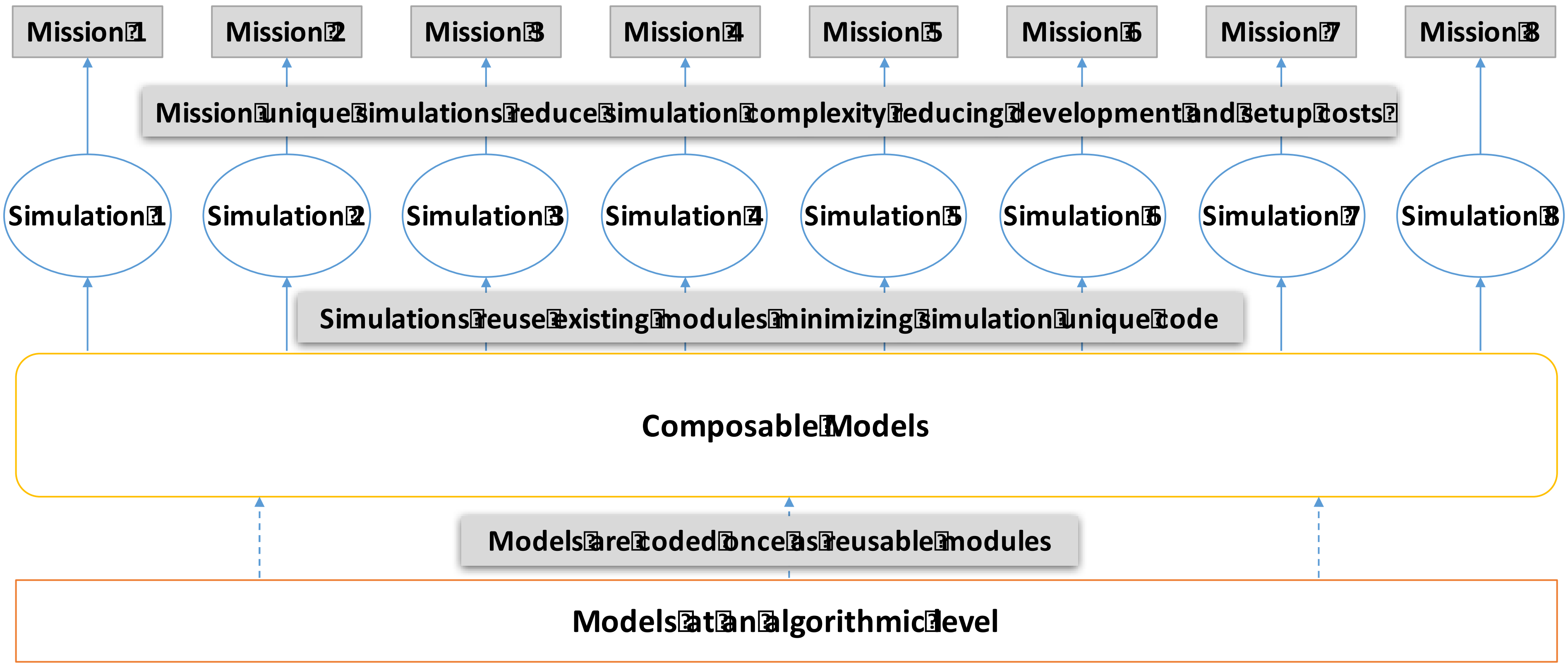
A robust modeling and simulation (M&S) capability that supports a full spectrum of DoD activities and operations, delivered to the point of need, within current fiscal constraints, managing schedules and risk enabled by agile composition.

- **Models and simulations that:**
  - Are modular – decomposed into loosely coupled reusable components;
  - Execute in the cloud (where practical) – hosted in the cloud, and are capable of taking advantage of cloud characteristics such as remote access and scalability;
  - Adhere to enterprise-wide composability standards – follow standards that facilitate the reusability of components across programs and Components.

OV-1 High Level Operational Concept Graphic



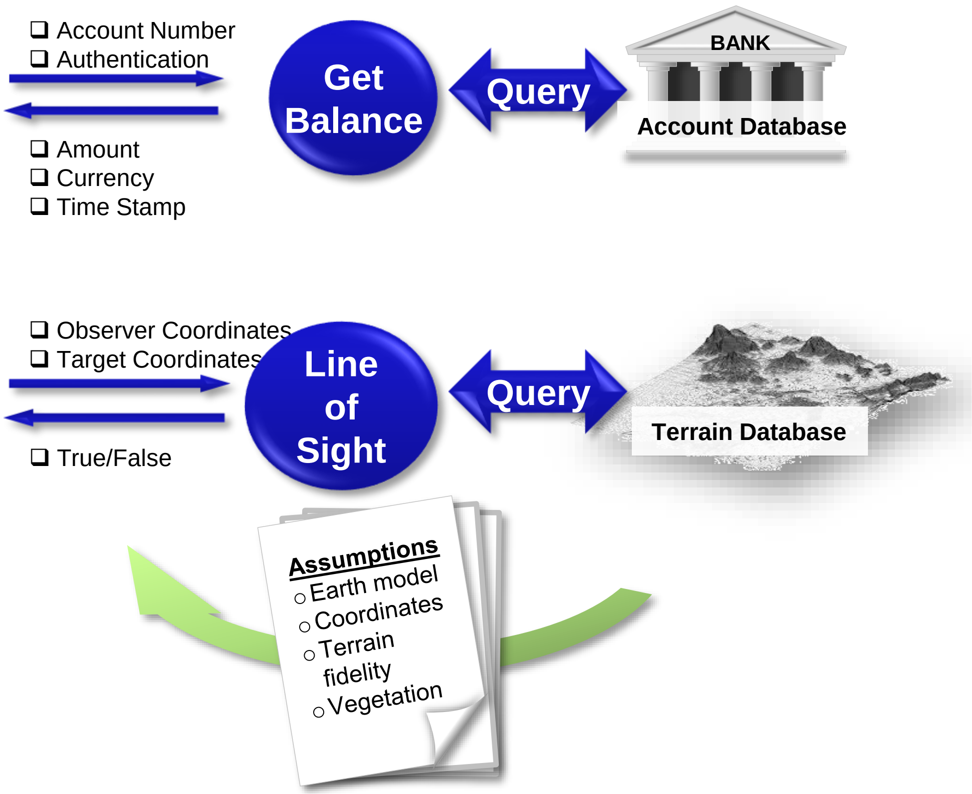
Composable Enterprise Architecture (EA)



Architectural and Engineering Challenges

- **Managing a hybrid architecture that maintains interoperability with legacy systems**
- **Decomposition of legacy systems into reusable components**
- **Development of standards to facilitate composability of models**
  - Common conceptual model/framework for assembling components
  - Verification and Validation of composed simulations

Unique M&S Challenges to Modular, Open System Approach



The bank keeps the <u>definitive</u> record of the amount of money in an account

The terrain database is a <u>representation</u> of the terrain based on a set of simplifying assumptions; those assumptions affect the suitability and accuracy of the data

Enterprise-wide Interoperability and Reuse Challenges

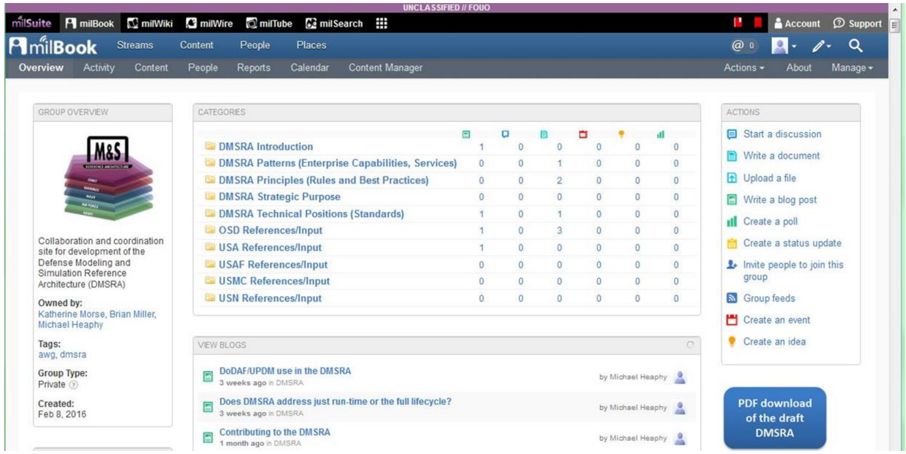
- **Implementing governance structures that enable and encourage modular, open-systems approaches**
- **Facilitating trust between simulation developers, dependent upon other model and simulation developers who may not be in their program chain.**
  - This will require simulation program managers to accept some risk
  - It will also require adoption of common conceptual model (s) or frameworks

How the DMSRA is Addressing the Challenges

- **Collaborative approach**
- **Leverage existing investments**
- **Develop patterns that capture best practices, and gaps in standards, technology and practice**

Collaborative Approach

- **M&S COI Architecture Working Group (AWG)**
  - 36 briefings on architecture / framework initiatives
  - Includes briefings from all 4 Services, MDA, Joint Staff, and NATO
  - Domains
    - ❖ Training
    - ❖ T&E
    - ❖ Acquisition
    - ❖ Experimentation
    - ❖ Analysis



- **Online collaboration**
  - Emphasizes the dynamic and collaborative nature of the DMSRA
  - Makes the revision process more transparent
  - Makes it easier to contribute to the DMSRA
  - Makes contributions immediately available and easier to find
  - https://www.milsuite.mil/book/groups/dmsra (DoD CAC only)

Leveraging Existing Investments

- **The DMSRA effort builds on the Live, Virtual, Constructive Architecture Roadmap (LVCAR) principles:**
  - Do no harm
  - Interoperability is not free
  - Start with small steps
  - Provide central management
- **Other investments and resources leveraged:**
  - Defense M&S Glossary
  - Verification, Validation, and Accreditation (VV&A) Recommended Practices Guide
  - DoD and NATO standards references and tools
  - Services' architecture(s) artifacts and practices

Patterns:
Best Practices and Gaps

- **Extensibility via Patterns**
  - The base document and initial patterns were not sufficiently comprehensive to meet the DMSRA vision
  - Led to the use of modular patterns to extend and evolve the DMSRA with new technologies and associated best practices.
- **DMSRA Pattern Outline:**
  - **Pattern overview:** Frames topic with definitions, technology description, and relevance to the DMSRA
  - **Mapping from Capabilities, and Principles and Rules:** aligns capability with DMSRA principles
  - **Pattern:** Provides a series of questions the user should ask in the process of deciding whether to apply the technology/capability. Documents guidance and best practices for answering the questions in context based on inputs from the AWG.
  - **Technical Positions:** Identifies applicable standards, including DoD adoption status; and standardization gaps
  - **References**

Current Patterns Findings (1 of 2)

- **Cloud migration**
  - Lower overall costs to the consumer, because of efficiencies obtained by pooling much of the computing hardware and software;
  - IT functions and increased flexibility because there is no upfront investment in infrastructure required by the end user
- **Service-oriented architecture**
  - The Department of Defense (DoD) Chief Information Officer (CIO) has directed the DoD to leverage commercial SOA technologies to reduce costs and increase flexibility.
  - This pattern aids the user to determine the suitability of an organizational capability for migration to a SOA from technical, programmatic, and domain perspectives.

Current Patterns Findings (2 of 2)

- **Decomposition of simulations into modular components**
  - Although much has been written about modular simulation, there is a gap for M&S-specific standard practices for decomposition.
- **Verification and validation of modular components**
  - Cloud computing considerations: The hardware and operating system the simulation is hosted on are out of the control of the user and may be altered from the configuration used during validation without the user's knowledge.
  - V&V of composed simulations: composition of validated component models does not ensure a valid composed simulation. This is a known gap in standards and practice.

Way Ahead

Continue collaborative approach to capturing best practices in patterns, including the following topics:

- **Accommodating occasional / sporadic connectivity**
- **Cross domain solutions**
- **Distributed simulation and federation engineering**
- **Data**
- **Assessing the feasibility of remote execution**
- **Gaming architectures**

Continue to leverage DoD enterprise architecture and IT capabilities and practices:

- **Cloud computing**
- **MOSA and SOA practices and standards**

QUESTIONS?

POTOMAC INSTITUTE FOR POLICY STUDIES

Developing Trust for a Secure Microelectronics Supply Chain

Dr. Mike Fritze

Senior Fellow

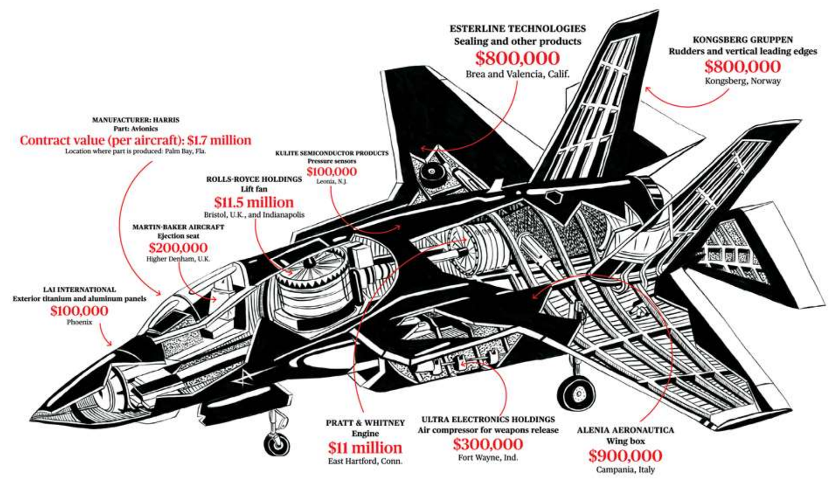
Potomac Institute for Policy Studies

Arlington, VA

Outline

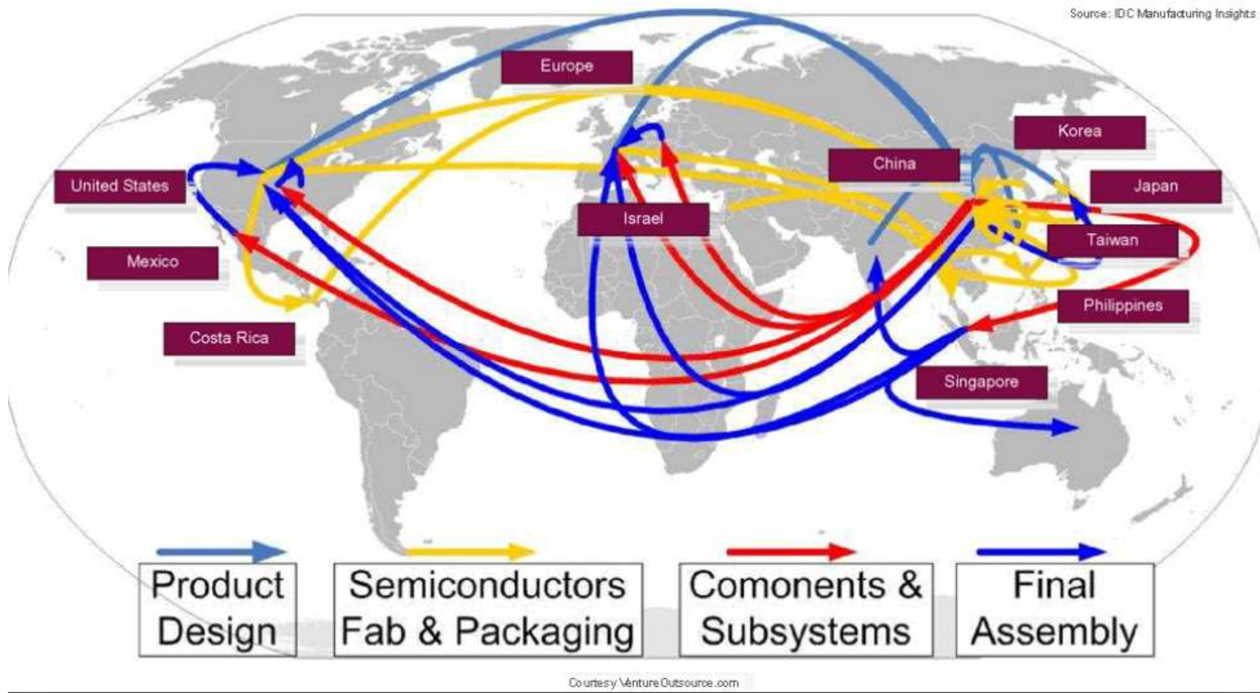
- Articulation of Trust Problem (for systems folks)
- Measuring Trust
- National Strategy for Trust

Defense Systems: Global Supply Chain



Increasing complexity in the supply chain results in decreased security of defense systems

Microelectronics Global Supply Chain



Supply Chain Lifecycle

Research & Design → Production (fabrication) → Supply, Stock & Store → Deployment

Threats to the Hardware Supply Chain

Hardware threats exist throughout the global microelectronics supply chain

The Supply Chain – From design and production to deployment
Malicious insertions, Counterfeits, Clones, Insider Threat

Research & Design
(Research, Development, Prototyping)

- Un-vetted 3rd party IP increases the number of people with knowledge of a design and provides opportunities to corrupt a design
- Zero Day effects can be embedded into a chip's design, go undetected, and be triggered after a chip has been produced

Production
(Fabrication)

- The U.S. is increasingly relying on off-shore foundries to supply components for our critical mission systems
- Only 2% of ASICs used in National Security Space systems come from DoD trusted foundries
- This increases the risk of malicious insertion to include Trojan horses, Kill Switches, and Backdoors

https://www.bloomberg.com/news/articles/2008-10-01/dangerous-fakes

Supply, Stock and Store
(Testing and Verification, Acquisition)

- Attack vectors exist throughout the entire supply chain to include – design, fabrication, testing, packaging, distribution, and end-of-life
- 53% of counterfeit incidents from 2003 – 2013 were for discontinued (legacy) components

Deployment
(Deployed mission systems, Logistics & Maintenance, end-of-life)

- Insider threats and counterfeits in the upgrade/refresh process
- Information exploitation
- Electronic warfare
- Kill switches and backdoors can be used
- Poor disposal practices

Measuring Hardware "Trust"

- "Trust" commonly used phrase but very difficult to precisely and quantitatively define

- **We propose an "insurance" based definition of Trust**

$$\mathbf{T=R/M}$$

T = level of trust; R = risk mitigation investment; M = mission value

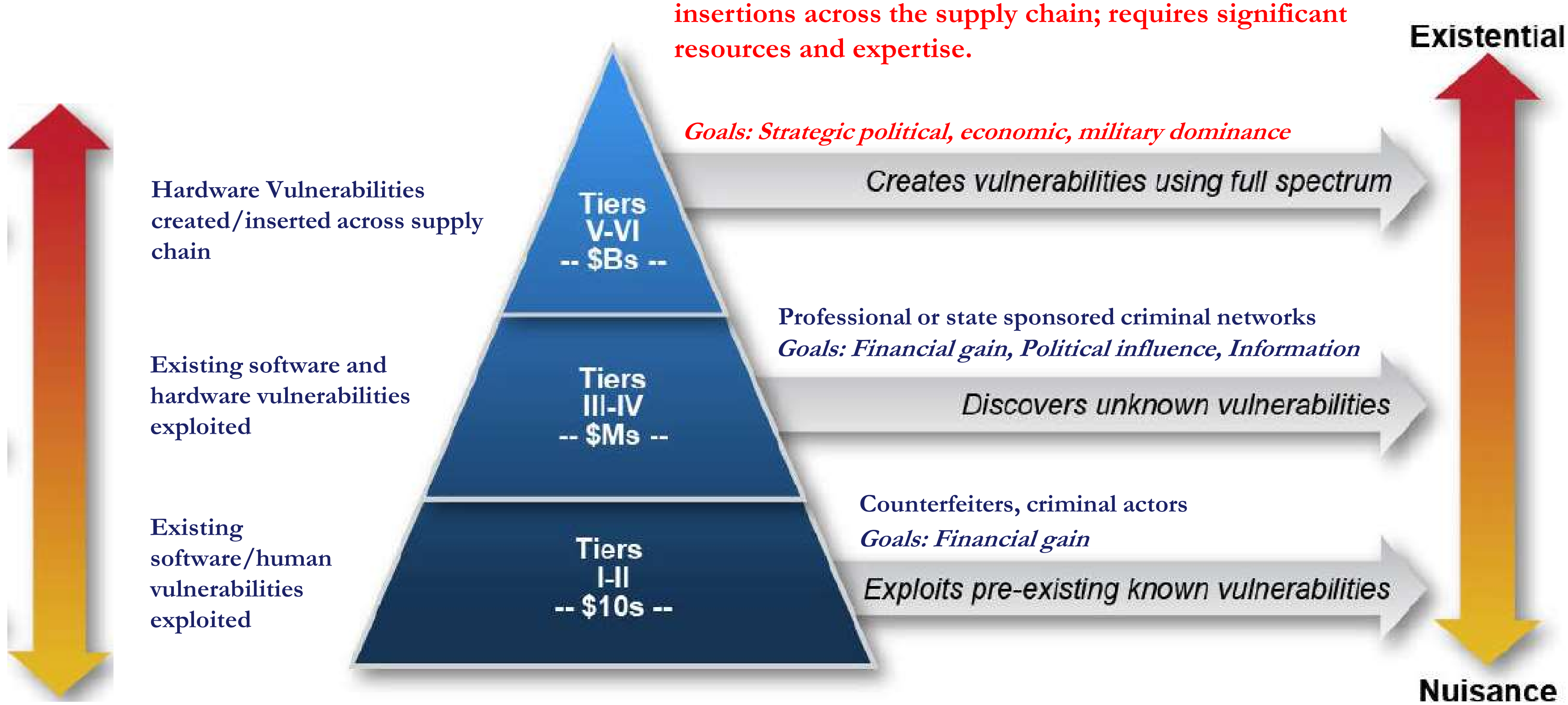
100% trust means we have mission "insured" for its full value

Insurance "purchased" depends on value of mission and nature of threats of interest

Relating Risks to Threat Type

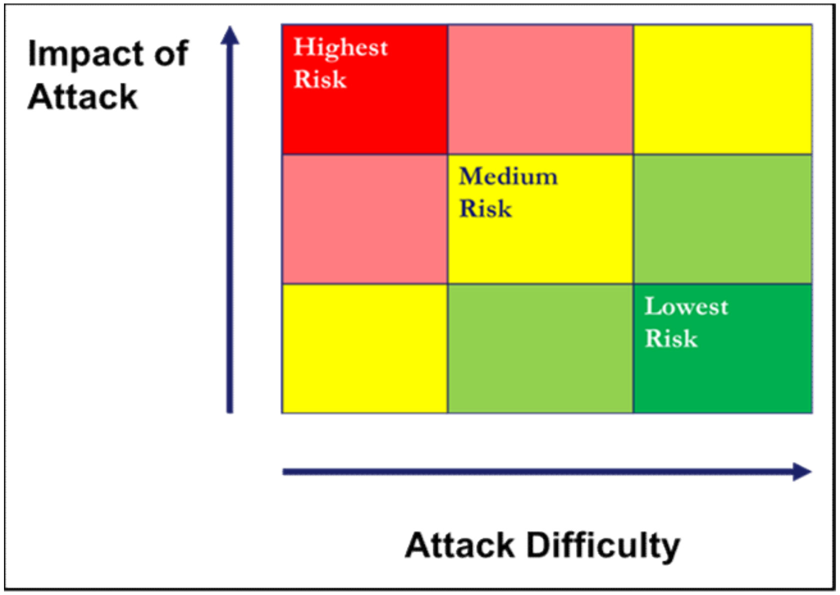
Anyone can hack software. It takes a nation state to attack hardware

Hardware attacks are by Nation state actors, capable of insertions across the supply chain; requires significant resources and expertise.



DSB Task Force Report: Resilient Military Systems and the Advanced Cyber Threat.
http://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

Mitigation Insurance: Impact vs Difficulty Matrix

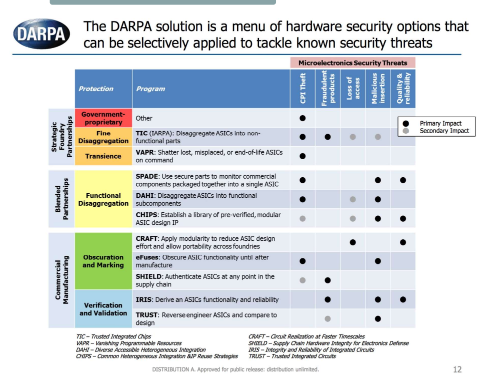


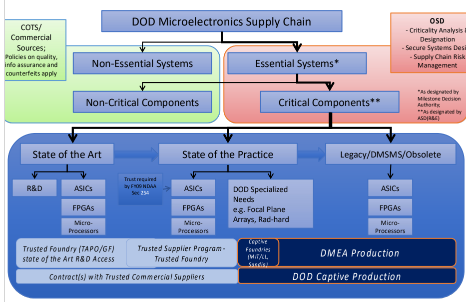
Mitigation "Insurance" Goal:
To make attacks more costly (difficulty/time/$) for the attacker than the defender

National Strategy: Address the entire supply chain
US Government Solution – DMEA Executive Agent

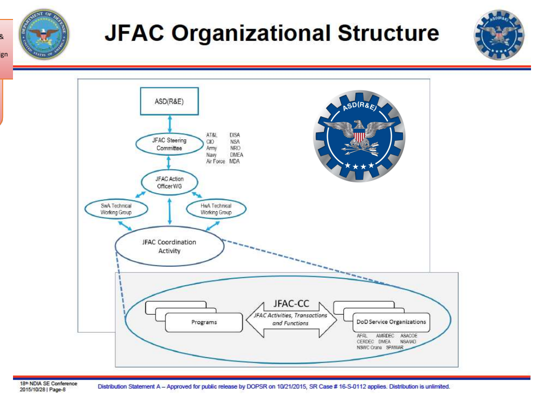
The Trusted Microelectronics Supply Chain

Research & Design → Production → Supply, Stock & Store → Deployment





Designate DMEA as Executive Agent



Current DoD Policies Include:

- Defense Industrial Base Sector Specific Plan (2010)
- Mission Assurance Strategy (2012)
- Antiterrorism Force Protection
- Counterfeit Mitigation Policies

National Strategy: Rationalizing & Integrating DoD Capabilities

The Trusted Microelectronics Supply Chain

Research & Design → **Production** → **Supply, Stock & Store** → **Deployment**

Research & Design

- Research for trusted design & manufacturing
- Manage relationship with Industry for R&D access to "pre-SOTA" technology
- Focus on research, design, and prototyping
- Acquisition of IP for pre-fab research

DARPA

Production

- SOTA → Trusted Foundry (GF)
- SOTP → Trusted Commercial Suppliers (79 Suppliers)
- Legacy → Flexible Foundry (DMEA)

Supply, Stock & Store

ASD(R&E)

↓

JFAC Steering Committee

- SwA Technical Working Group
- HwA Technical Working Group

Deployment

Armed Services need new policies to secure deployed systems

Field Programmable Gate Array (FPGA) Assurance

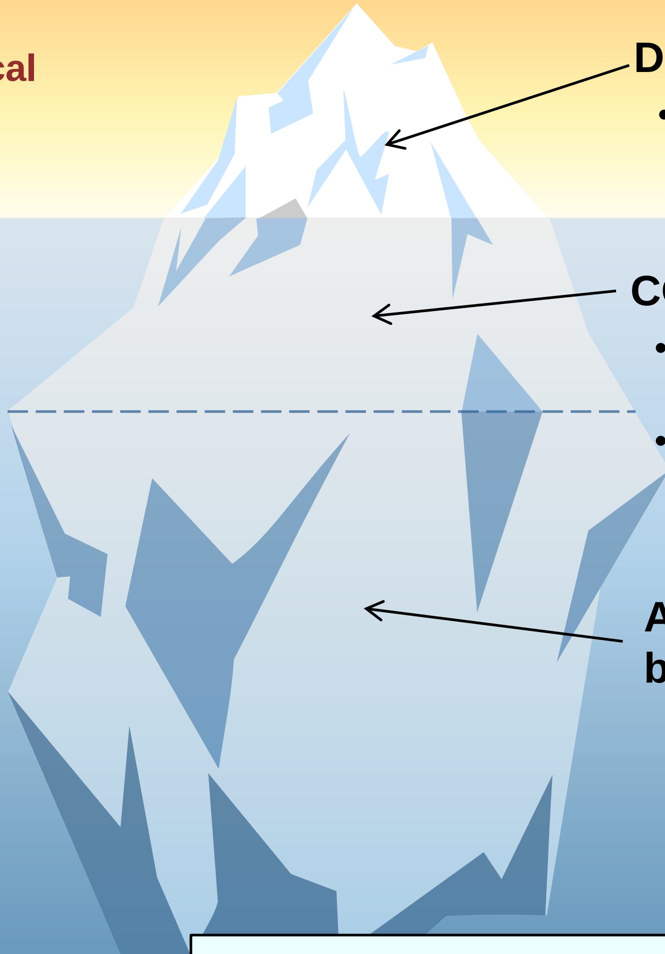
Raymond C. Shanahan
Deputy Director, Anti-Tamper/Hardware Assurance
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 26, 2017

Electronics as a Strategic Issue

Current Tactical Issue

Larger Strategic Issue



DoD Trusted Electronics Issue

- **Options for domestic trusted manufacture of custom DoD electronics are diminishing**

FY03-present: DoD Trusted Foundry Program

COTS Electronics Assurance (DoD & Beyond†)

- **Most COTS electronics used in DoD systems are fabricated overseas; significant risk from tamper**
- **Risks similar for the broader national security community, banking, critical infrastructure, etc.**

PB 2017: Trusted & Assured Micro-electronics

Access to Electronics / Electronics-based economic growth

- **Shift in electronics fabrication creates potential for overseas control**
- **End of Moore's Law potential carries economic impacts**

PB 2018/ POM 19: Microelectronics Innovation for National Security and Economic Competitiveness

Significant electronics challenges represent a strategic level national issue

† Including the broader national security community, banking, critical infrastructure, commercial industry, etc.

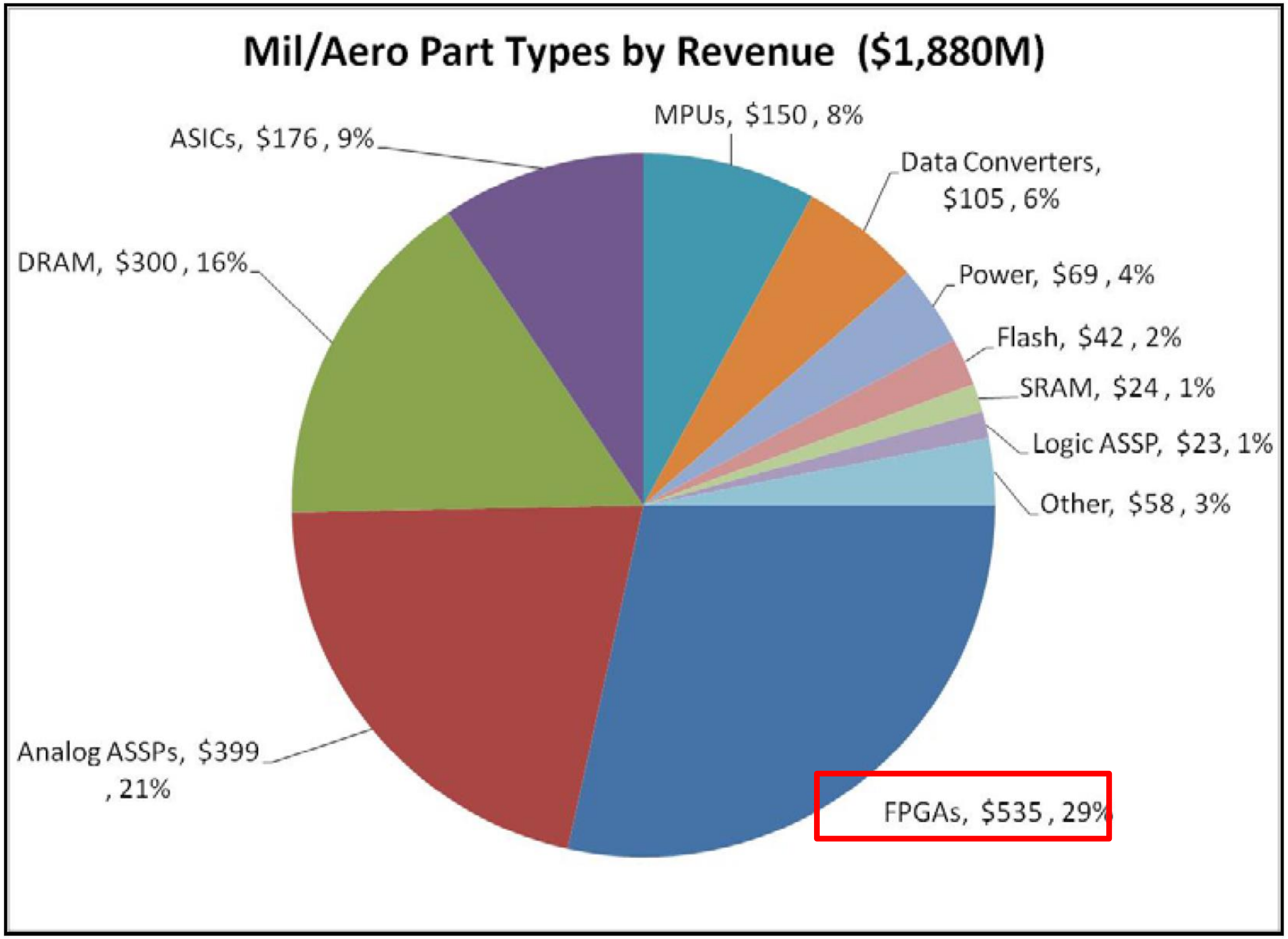
Need for Assured FPGA Functionality

- **Commercial FPGAs are in widespread use across National Security Systems (NSSs) in embedded, special purpose applications**
  - Programmable nature of FPGAs and System on Chips (SOCs) make them vulnerable to cyber malware and malicious insertion
- **While Application-Specific Integrated Circuits (ASICs) have performance of ten to a thousand times that of FPGAs, FPGAs are seen as achieving custom hardware performance without the high manufacturing cost of custom ASICs**

FPGA applications:

- Communication systems
- UAVs
- Tactical robotics
- Radar systems
- Missile control
- Satellites
- Ships
- Vehicle control systems
- Other

FPGA Usage by Revenue in Military/Aerospace Sector



Source: IDA report, Examination of DoD's Use of Microelectronics in Weapon Systems, 2013

Policy Requirement for Trust vs. Assurance

- **There is no policy requirement in DoDI 5200.44 for a Trusted FPGA or other COTS product; only ASICs as follows:**
  - "In applicable systems, integrated-circuit-related products and services shall be procured from a trusted supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASIC))."
- **However, there are policy requirements for assurance in DoDI 5200.44, to include the following of particular relevance to FPGAs:**
  - "Mission critical functions and critical components within applicable systems shall be provided with assurance consistent with criticality of the system, and within their role within the system."
  - "Control the … security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources. Employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use."
  - "Detect the occurrence of, reduce the likelihood of, and mitigate the consequences of unknowingly using products containing counterfeit components or malicious functions in accordance with DoDI 4140.67"
  - "Detect vulnerabilities within custom and commodity hardware and software through rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing"

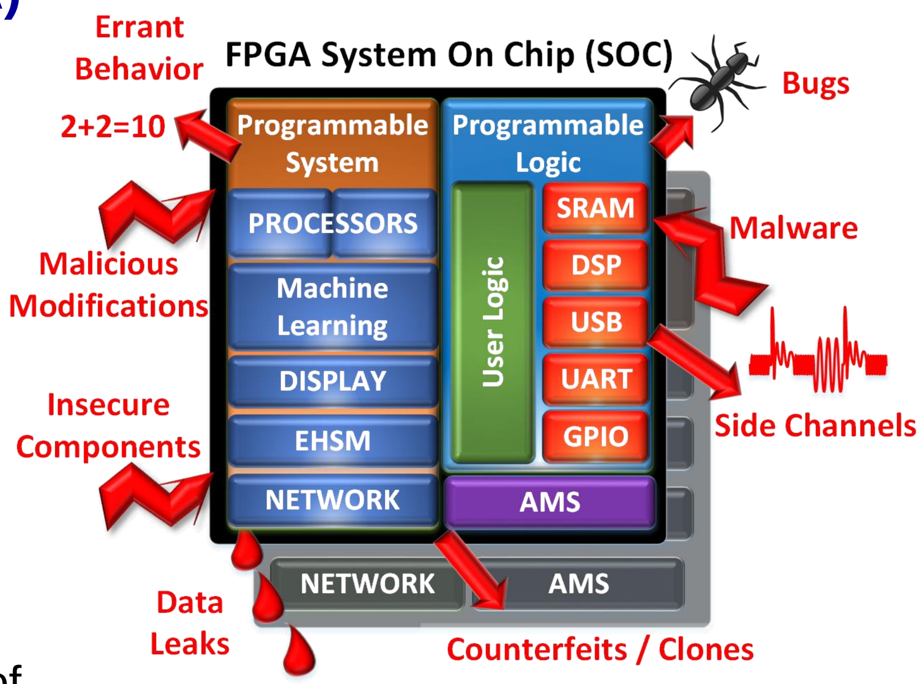
Definitions of Trust and Hardware Assurance

- **The NDAA FY2017 Sec. 231 trust definition below reflects DASD(SE)'s working definition of the term, "hardware assurance (HwA)"**
  - The other trust definition below is used by the DoD Trusted Foundry Program
- **Planned update of DoD Instruction (DoDI) 5200.44 needs to add, clarify, and harmonize the definition(s) of HwA and/or trust**
  - Needed to eliminate existing confusion in the community between what constitutes trust versus HwA; sometimes referred to as "big T" versus "little T" trust or assurance
  - These definitions do not compete with one another, but can be complementary if integrated and harmonized into an internally consistent definition or set of definitions within DoDI 5200.

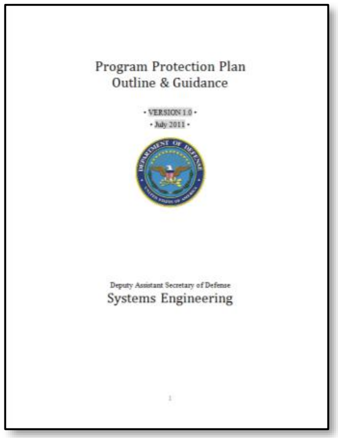
2004 AT&L Memorandum	NDAA FY2017 Sec. 231
trust: "the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture and distribute national security critical components"	**trust:** "with respect to microelectronics, to the ability of the Department of Defense to have confidence that the microelectronics function as intended and are free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during its lifecycle"

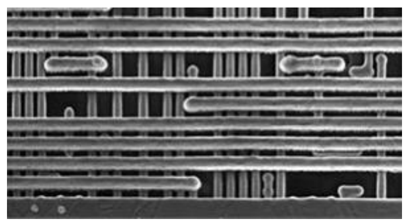
FPGA/SOC Assurance Risks

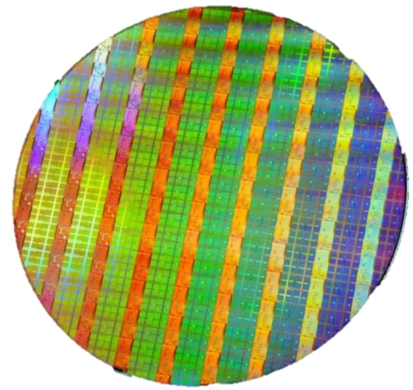
- **Commercial FPGA/SOC security, third party intellectual property (3PIP), and Electronic Design Automation (EDA) tools are largely unverified**
- **Industry unlikely to invest unless encouraged**
- **Some Military/Aerospace and specialty needs are not being met**
- **DoD uses FPGAs heavily in critical systems and many potential vulnerabilities exist**
  – Potential for compromise of IP confidentiality and/or integrity, or EDA tool integrity, from design through deployment
  – Inconsistencies and uncertainty/lack of clarity in methods, policy, and enforcement
  – Supply chain threat and vulnerability awareness is poor

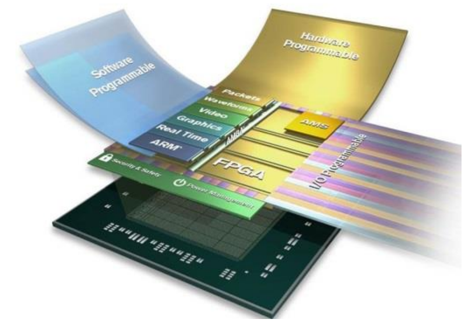


Advancing Hardware Assurance


Program Protection Plan
Outline & Guidance
VERSION 1.0
July 2011
Deputy Assistant Secretary of Defense
Systems Engineering







Policy

- DoD Instruction (DoDI) 5000.02
- Program Protection Plan (PPP)
- International Traffic in Arms Regulations (ITAR) update (in work)

Joint Federated Assurance Center

- Software assurance Know-how & tools
- Hardware assurance Know how & tools
- Advanced V & V capabilities
- Firmware Assurance planning

Trusted & Assured Microelectronics

- Access to state-of-the-art foundries
- Trust and assurance methods and demonstration
- Industrial best practices for assurance
- Implement & Demo

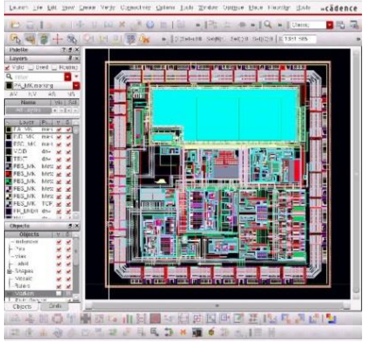
COTS and FGPA

- Supply chain risk management
- FPGA Assurance Strategy
- Radiation hardened microelectronics initiative

Microelectronics Trust Verification Technologies

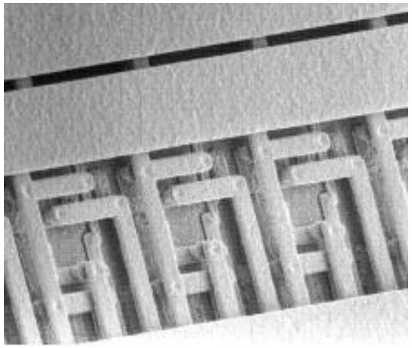
Design Verification

- Verification/assurance of designs, IP, netlists, bit-streams, firmware, etc.



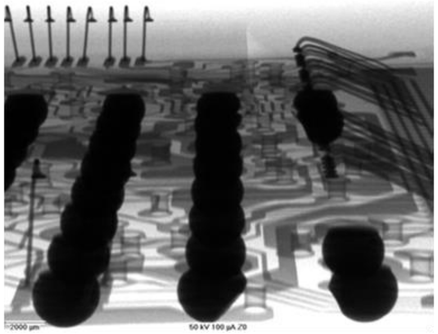
Physical Verification

- Destructive analysis of ICs and Printed Circuit Boards



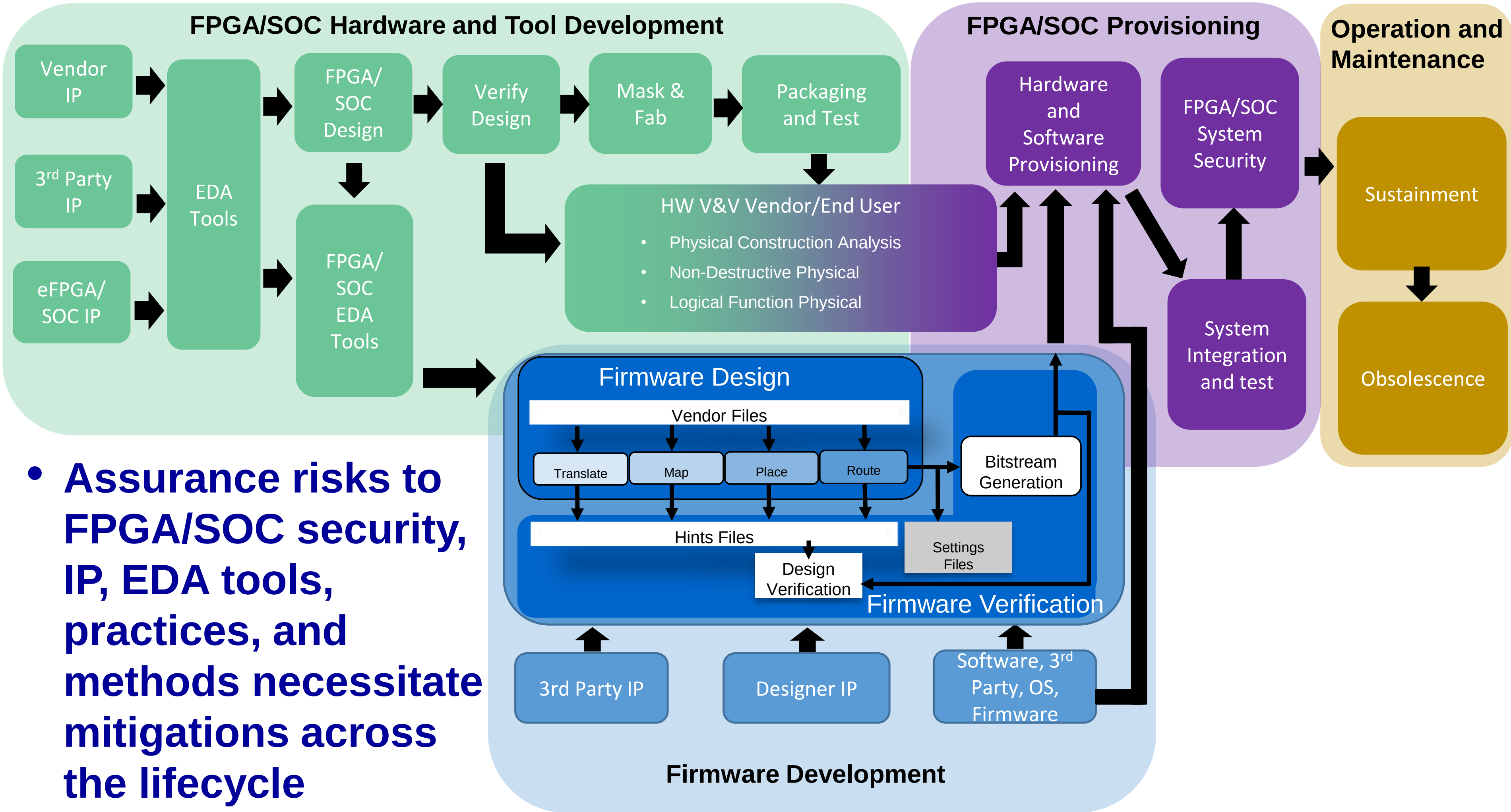
Functional Verification

- Non-destructive screening and verification of select ICs



DoD, Intelligence Community, and DoE enhancing capability to meet future demand

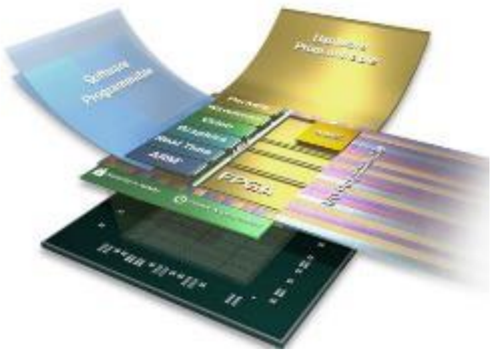
FPGA/SOC Lifecycle Map



- **Assurance risks to FPGA/SOC security, IP, EDA tools, practices, and methods necessitate mitigations across the lifecycle**

FPGA Assurance Strategy Overview

- **DASD(SE) continues to refine the strategy to address FPGA assurance risks in coordination with the Joint Federated Assurance Center (JFAC) HwA Technical Working Group (TWG) and the Trusted and Assured Microelectronics (T&AM) program**
  - Leverage existing USG and industry efforts to the maximum extent possible
  - Promote community awareness of related USG efforts via a series of workshops and conference
  - As a community, continuing to identify and refine the portfolio of assurance efforts to focus on with the goal of synchronizing and eliminating stove-pipes and separate, single-point solutions when possible
  - Identify gaps and/or activities requiring investment and elevate relevant needs to the JFAC Steering Committee for prioritization and direction regarding resourcing
  - In particular, align with, and inform, the execution plan for the T&AM program



FPGA Assurance Strategy has multiple FPGA Assurance Focus Areas across the FPGA Lifecycle

		FPGA/SoC Hardware Development	FPGA/ Firmware Development	FPGA/SoC Provisioning	Operation & Maintenance
AVAILABILITY	DoD Specific Needs	Increase availability for DoD specific needs in Military/Aerospace, e.g., Strategic Radiation-Hardened (SRH) technologies, and other domestic manufacturing needs			
	Leverage Related Efforts	Coordinate with other major efforts across the DoD, Intelligence Community (IC), the broader United States Government (USG), industry, and academia. For example: • Defense Production Act (DPA) Title III Trusted FPGA • Trust in FPGA Studies • Aerospace Terms of Reference (TOR) related to assured FPGA and ASIC development			
ACCESS	Supply Chain Threat	Enhanced interaction with the IC to provide more specific threat information to enable enhanced threat assessment and vulnerability analysis			
	Industry Engagement	Engage FPGA manufacturers, EDA, 3PIP, and other vendors to facilitate: • USG IV&V access to timely/detailed supply chain information, e,g., design, chain of custody, etc. • Design tool and 3PIP distribution and enterprise usage • Verification features in the design or that are enabled by the design tools • Commercial verified and validated security features, EDA tools, 3PIP or other supply chain tools			
	Policy and Guidance (P&G) and Standards	Develop, contribute to, and/or adopt P&G and standards that promote best practices across DoD and other USG acquisition programs as well as industry to the extent possible • Facilitate use of commercially viable/supportable tools, IP, and best practices where possible			
ASSURANCE	Independent Verification And Validation (IV&V)	Expand JFAC IV&V capability and capacity for physical, functional and design V&V to be offered to clear contractors and USG acquisition programs, leverage co-development, data access, design for assurance, and other best practices to enable better V&V			
	New HwA Techniques and Tools	Develop and facilitate the transition of new HwA techniques and tools to verify and validate, protect the confidentiality and integrity of, and gain insight into the chain of custody of, IP, EDA tools, and the FPGAs/SOCs themselves			

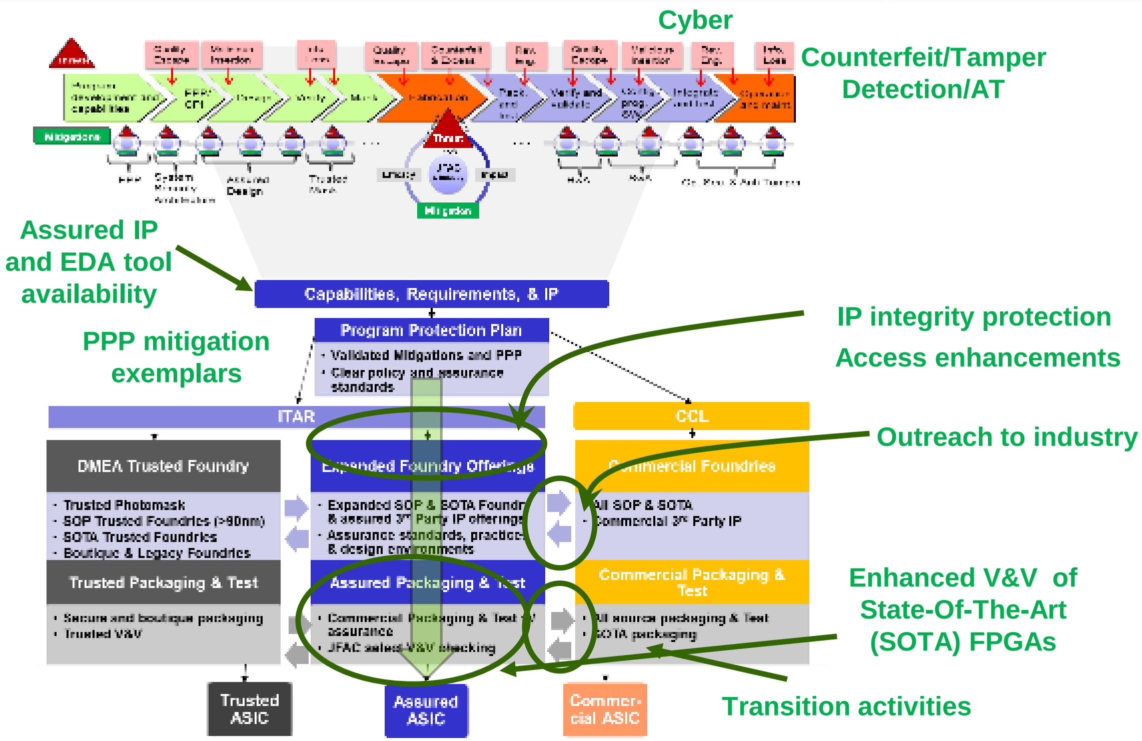
FPGA Activities and Investments

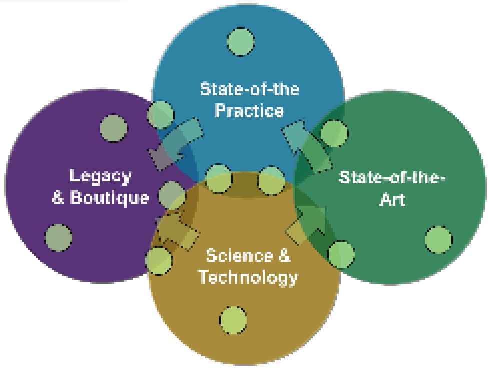
Overall

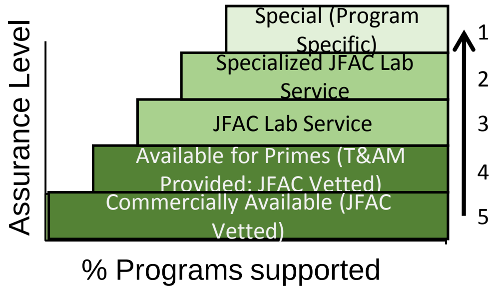
Inputs	Investments & Actions	Outcomes
• Established relationships and programs with FPGA and other vendors • JFAC labs, FFRDCs, expertise • Other USG partners and commercial suppliers • Programs and COTS parts	• EDA tool and 3PIP V&V development • Physical V&V tool and capability development • Security and assurance architecture development • Radiation testing and validation	• USG and third party EDA and 3PIP V&V tools • JFAC-assessed FPGA list, IV&V tools, vulnerability assessments • Counterfeit and SCRM tools • P&G, standards, and best practices, PPP • SRH assessments

Investment Breakout

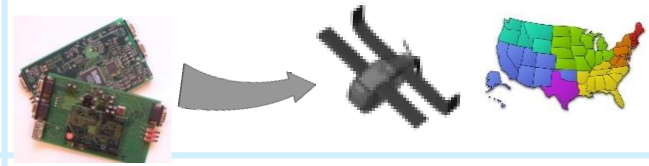
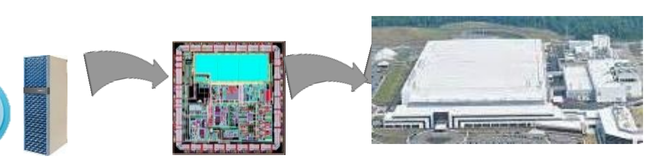
15.0%	18.9%	66.0%
Availability	Access	Assurance







FPGA Strategy Outcomes

	Problem	Actions & Investments	Outcomes
Availability	• DoD influence is limited and national security needs not satisfactory for required production and volume	• Support domestic, manufacturing of SOTA FPGAs and industrial engagement for USG and strategic growth application areas, including radiation-hardening, high voltage, etc.	• Availability of assured SOTA FPGAs, tools, and IP for USG acquisition programs 
Access	• Potential for compromise to confidentiality and integrity through design access, COTS insertion, and deployment of commercial FPGA creates risk when USG accesses SOTA FPGA	• Evaluate and adopt best practices, and specialized tools and services to assure integrity and confidentiality of IP	• Enhanced USG access to assured SOTA FPGAs, IP, and EDA tools 
Assurance	• DoD uses FPGAs heavily in critical systems and many potential vulnerabilities exist	• Provide USG HwA community with access to, or knowledge of, assured USG IP, 3PIP, EDA tools, experts, secure computing, techniques, etc. for innovation 	• Assurance throughout the FPGA/ SOC lifecycle through secure design environments, best practices, V&V and supply chain tools, and specialized services 

Leverage Related Efforts

- **Trust in FPGA Studies**
- **JFAC HwA TWG efforts**
- **Defense Production Act (DPA) Title III Trusted FPGA Projects**
  - In FY17, DPA Title III Phase 1 worked with FPGA vendors to develop product strategies to allow USG to assure FPGAs
  - In FY18, Phase 2, planned start of implementation of those product strategies
- **Defense Microelectronics Activity (DMEA) Trusted FPGA Study**
  - Congressional Add to engage major vendors
- **Anti-Tamper Executive Agent-related technology development**
- **Printed Circuit Board and Interconnect Technology Executive Agent technology development**

Leverage Related Efforts (cont'd)

- **NSA/R2-sponsored FPGA Trust & Integrity Research**
  - Aerospace documenting this research. Final product in FY17
- **Mission Assurance Improvement Workshop (MAIW) and Aerospace Terms of Reference (TOR)**
  - FPGA assurance-related TORs for design, Trust Assurance, and SME training in development
  - Other FPGA and ASIC related TORs already completed
- **National Defense Industrial Association FPGA Assurance Workshops**
- **Intelligence Advanced Research Projects Activity Trusted Integrated Circuit (TIC) Phase 3**
  - FPGA developed using split fabrication
- **Defense Advanced Research Projects Agency programs**

FPGA
Oct 26, 2017| Page-16

The Way Ahead

- **Program engagement**
  - Foster early planning for HwA and SwA, design with security and assurance in mind
  - Implement expectations in plans and on contract
  - Support vulnerability analysis and mitigation needs
- **Community collaboration**
  - Achieve a networked capability to support DoD needs: shared practices, knowledgeable experts, and facilities to address malicious supply chain risk
- **Industry engagement**
  - Communicate strategy to tool developers and develop standards for common articulation of vulnerabilities and weaknesses, capabilities and countermeasures
  - Co-development of next generation COTS with DoD capabilities and assurance considered
- **Advocate for R&D**
  - HwA and SwA tools and practices
  - Strategy for trusted microelectronics, to include FPGAs/SOCs, that evolves with the commercial sector
- **People!**
  - Improve awareness, expertise to design and deliver trusted systems

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace

http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering

http://www.acq.osd.mil/se

For Additional Information

Raymond C. Shanahan

Deputy Director, Anti-Tamper/ Hardware Assurance

ODASD, Systems Engineering

571-372-6558

raymond.c.shanahan.civ@mail.mil

E-mail – osd.pentagon.ousd-atl.mbx.fpga-assurance@mail.mil

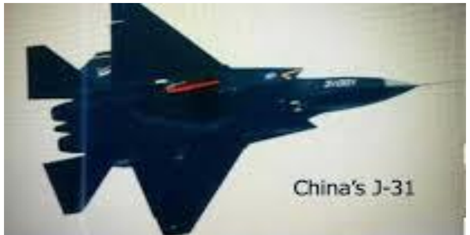
JFAC Portal -- https://jfac.army.mil

Engaging the DoD Enterprise to Protect U.S. Military Technology Advantage

Brian Hughes
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

These are Not Cooperative R&D Efforts



M-16

QBZ-95

Reaper

Yìlóng-1

HUMVEE

Dongfeng EQ2050

Case History: Titanium Dioxide

Walter Liew, a naturalized American citizen, business owner, and technology consultant stole DuPont's protocols for producing its superior titanium white from 1997 through 2011

- DuPont developed $2.6B per annum Titanium Dioxide business – recognized as world leader
  - Processes created in 1940s but spent $150M year to improve processes by 1%
    - Near monopoly on the manufacturing techniques
  - Shielded its titanium dioxide process
    - Guards
    - Escorted Visitors
    - Documents and blueprints controlled
  - Starting in 1990's China began seeking ways to illegally acquire DuPont's methods
    - China accounts for approximately 25% of the demand

Liew was convicted in 2014 on each of twenty counts with which he was charged and sentenced to serve 15 years in prison, forfeit $27.8 million in illegal profits, and pay $511,667.82 in restitution

Bottom Line Up Front

- Adversary is targeting our Controlled Technical Information (CTI)
- DoD is emphasizing protection activities to encompass the full range of threats and vulnerabilities across the acquisition life cycle
- The Joint Acquisition and Protection and Exploitation Cell (JAPEC) enables a comprehensive analysis of protections for DoD's critical programs and technologies (CP&T) and addresses shortfalls
- Significant amount of technical expertise resides in the Defense Industrial Base (DIB)
- The DIB is not only critical to protecting that information but helping DoD identify which information it should protect

Partnership between DoD and DIB is vital

Agenda

- **DoD Efforts to Safeguard Controlled Technical Information (CTI)**
- **Know the Environment**
- **Stakeholder Dialogue**
- **Defense Industrial Base (DIB)'s Role in the Process**

Addressing the Loss of CTI

Risk = f (threat, vulnerabilities, consequences)

Goals:

- **Enable information-sharing, collaboration, analysis, and risk management between acquisition, Law Enforcement (LE), Counterintelligence (CI), and Intelligence Community (IC)**
  - Connect the dots in the risk function (map blue priorities, overlay red threat activities, warn of consequences)
- **Integrate existing acquisition, LE, CI, and IC information to connect the dots in the risk function - linking blue priorities with adversary targeting and activity**
  - Many sources and methods are relevant (e.g., HUMINT, joint ventures)
  - Cyber is only one data source
- **Focus precious resources**
- **Speed discovery and improve reaction time**
- **Ultimately, evolve to a more proactive posture**

JAPEC Mission: Integrated Analysis

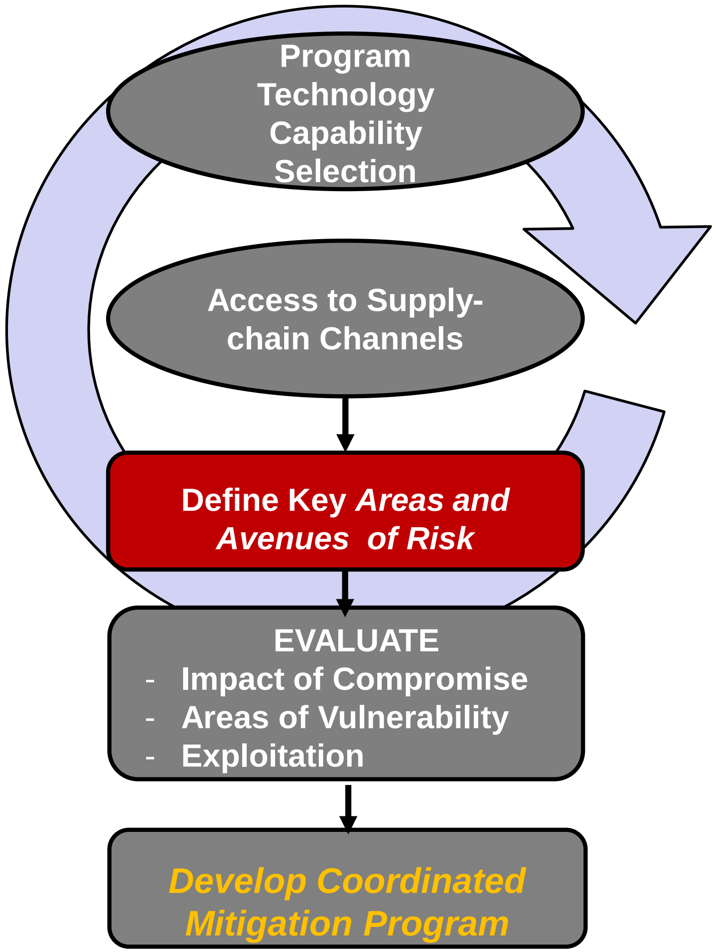
The Joint Acquisition and Protection and Exploitation Cell (JAPEC) integrates and coordinates analysis to enable Controlled Technology Information (CTI) protection efforts across the DoD enterprise to proactively mitigate future losses, and exploit opportunities to deter, deny, and disrupt adversaries that may threaten US military advantage.

Identifying Critical Programs and Technologies for Proactive Protection

ACQUISITION
- Identify DoD's Critical Acquisition and Technology
- Link technologies across the enterprise
- Identify protection methods
- Educate the workforce

SECURITY
- Integrate CI/Security posture
- Coordinated Security Classification Guides
- Onsite protection at DIB
- Contractor threat education

COUNTERINTELLIGENCE/ LAW ENFORCEMENT
- Collect against adversary activity
- Field presence
- Facility security analysis
- CI threat assessment
- Investigations & Prosecution



REQUIREMENTS
- Revise requirements based on change in threat

INTELLIGENCE
- Identify adversary technologies needs

DIB
- Understand Supply Chain
- Proactive approaches
- Improve Information Sharing w/ DoD

CIO/NETWORK SECURITY
- Tiered IT security controls
- Enroll in threat sharing forums

JAPEC projects demonstrated the effectiveness of an integrated iterative approach.
JAPEC methods complement other DoD efforts.

Agenda

- DoD Efforts to Safeguard Controlled Technical Information (CTI)
- **Know the Environment**
- Stakeholder Dialogue
- Defense Industrial Base (DIB)'s Role in the Process

Understanding Your Supply Chain

- **Increase level of concern for DoD's protection priorities throughout the supply chain**
  - Includes vendors, mergers, acquisitions, subsidiaries
- **Executive Order on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States dtd 21 July 2017**
- **Within 270 days**
  - (a) identifies military and civilian materiel, raw materials, and other goods essential to national security;
  - (b) identifies manufacturing capabilities essential to producing goods identified pursuant to subsection (a) of this section, including emerging capabilities;
  - (c) identifies defense, intelligence, homeland, economic, natural, geopolitical, or other contingencies that may disrupt, strain, compromise, or eliminate supply chains of goods identified pursuant to subsection (a) of this section (including as a result of the elimination of, or failure to develop domestically, capabilities identified pursuant to subsection (b) of this section) and that are sufficiently likely to arise so as to require reasonable preparation for their occurrence;
  - (d) assesses resiliency and capacity of manufacturing and defense industrial base and supply chains of the United States to support national security needs

How well do you know your supply chain?

Agenda

- DoD Efforts to Safeguard Controlled Technical Information (CTI)
- Know the Environment
- **Stakeholder Dialogue**
- Defense Industrial Base (DIB)'s Role in the Process

Dialogue with Protection Stakeholders

- **Compliance with existing rules & regulations is necessary but not sufficient**
  - Protection is more than completing a checklist
- **What is crucial to your organization delivering the desired capability?**
  - Identify who, what and where at each facility
    - FSO may not be well positioned to speak to this
  - Are there links with other programs, especially if programs are in a different Military Department?
    - Informing all involved parties helps focus IC, CI, and LE resources
  - Are there plans to market the same technology to other Military Departments or Government Agencies?
    - Government regulations and laws protect business proprietary
- **DoD/DIB information sharing improves the US' ability to focus priorities on most critical technologies**
  - Timely reporting to DoD which includes more than cyber incidents
  - Information sharing forums enable you to learn from other's experiences

Adversary is Dynamic and Active

Agenda

- DoD Efforts to Safeguard Controlled Technical Information (CTI)
- Know the Environment
- Stakeholder Dialogue
- **Defense Industrial Base (DIB)'s Role in the Process**

DIB Role

- **Identify crucial elements for protection up front**
  - Requires coupling technical know how with CI/LE expertise
  - Develop and implement training that focuses specifically on CTI handling and protection requirements
- **Do you have your own list of technologies crucial to you?**
- **Report**
  - Cyber incidents
  - Suspicious contacts
  - Media Theft and Loss
  - Insider Threats
- **Consider joining the DIB CS program**
  - Enables Government to Industry information sharing
  - Join and contribute to the DIB CS program at http://dibnet.dod.mil/
  - Share cyber forensic reports with DoD
- **Maintain an open dialogue with all the protection stakeholders**
  - Counterintelligence, Law Enforcement, Network Security, etc.
  - Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting at http://www.dss.mil/documents/ci/2017_CI_Trends_Report.pdf

The DIB is a critical partner in preventing unauthorized access to precious U.S. intellectual property and manufacturing capability by adversaries

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

Questions

Mr. Brian D. Hughes

Director, Joint Acquisition Protection and Exploitation Cell (JAPEC)

brian.d.hughes3.civ@mail.mil

571-372-6451

Engineering
Cyber Resilient Weapon Systems

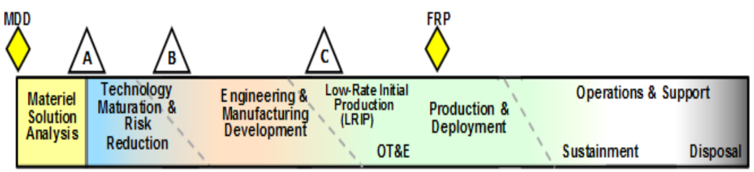
Melinda K. Reed
Office of the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

Ensuring Cyber Resilience in Defense Acquisition Systems

- ***Threat:***
  - Adversary who seeks to exploit vulnerabilities to:
    - Acquire program and system information;
    - Disrupt or degrade system performance;
    - Obtain or alter US capability
- ***Vulnerabilities:***
  - Found in programs, organizations, personnel, networks, systems, and supporting systems
  - Inherent weaknesses in hardware and software can be used for malicious purposes
  - Weaknesses in processes can be used to intentionally insert malicious hardware and software
  - Unclassified design information within the supply chain can be aggregated
  - US capability that provides a technological advantage can be lost or sold
- ***Consequences:***
  - Loss of technological advantage
  - System impact – corruption and disruption
  - Mission impact – capability is countered or unable to fight through

Access points are throughout the acquisition lifecycle…



…and across numerous supply chain entry points

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

Key Protection Activities to Improve Cyber Resiliency

Program Protection & Cybersecurity

DoDI 5000.02, Enclosures 3 & 14

DoDM 5200.01, Vol. 1-4 **DoDM 5200.45** **DoDI 8500.01**

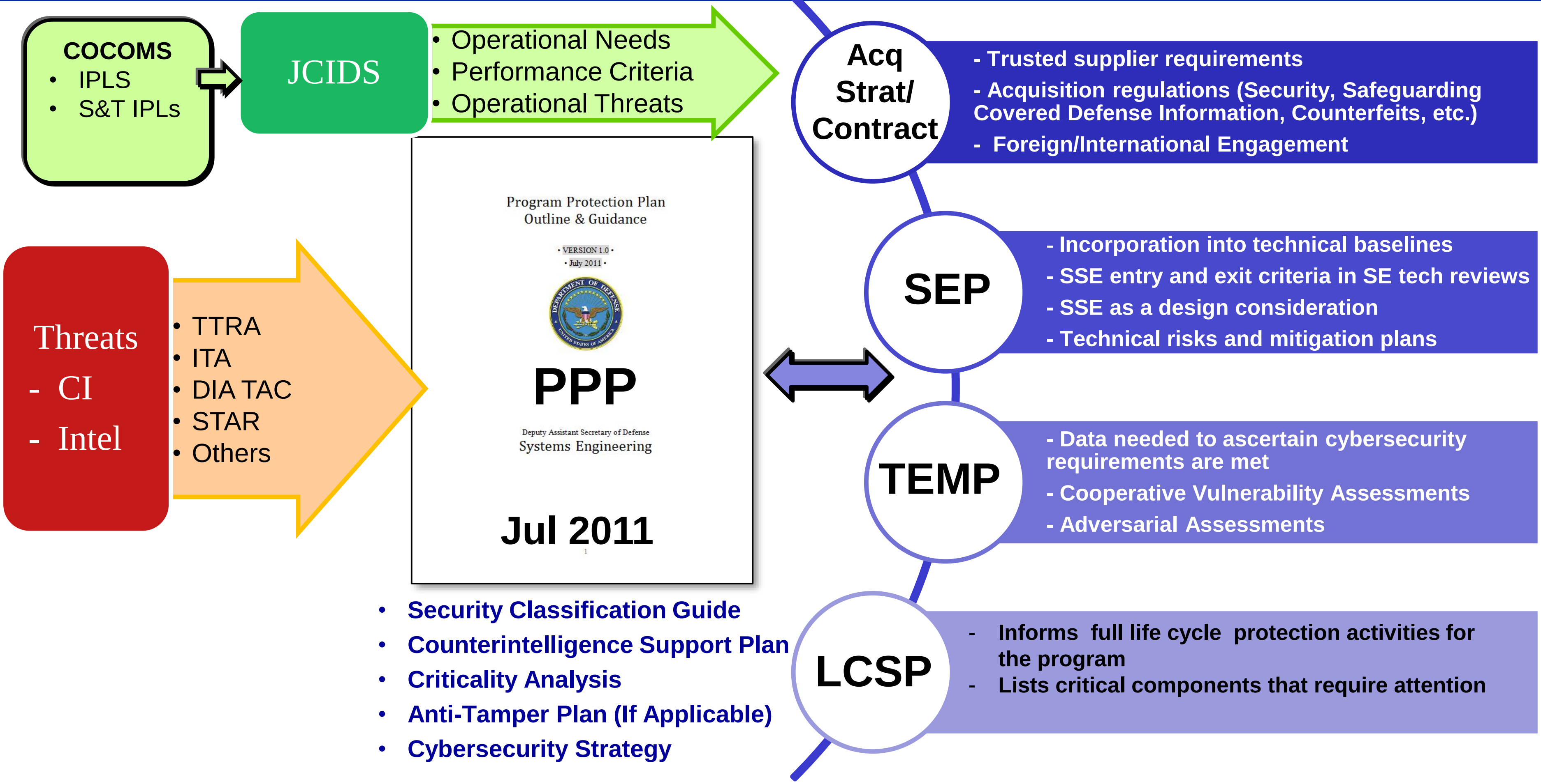
DoDI 5200.39 **DoDI 5200.44** **DoDI 5230.24** **DoDI 8510.01**

Technology	Components	Information
What: A capability element that contributes to the warfighters' technical advantage (Critical Program Information (CPI))	**What:** Mission-critical functions and components	**What:** Information about the program, system, designs, processes, capabilities and end-items
Key Protection ActivityU • Anti-Tamper • Defense Exportability Features • CPI Protection List • Acquisition Security Database	**Key Protection Activity:** • Software Assurance • Hardware Assurance/Trusted Foundry • Supply Chain Risk Management • Anti-counterfeits • Joint Federated Assurance Center (JFAC)	**Key Protection Activity:** • Classification • Export Controls • Information Security • Joint Acquisition Protection & Exploitation Cell (JAPEC)
Goal: Prevent the compromise and loss of CPI	**Goal:** Protect key mission components from malicious activity	**Goal:** Ensure key system and program data is protected from adversary collection

Protecting Warfighting Capability Throughout the Lifecycle

Policies, guidance and white papers are found at our initiatives site: https://www.acq.osd.mil/se/initiatives/init_pp-sse.html

Program Protection and Cybersecurity Relationship to Key Acquisition Activities



Program Protection and Cybersecurity Considerations Are Integrated In All Aspects of Acquisition

Cybersecurity Is Everyone's Responsibility

Cybersecurity is not just an IT / network issue. We must translate Cyber IT / Network practices, standards, etc. into physical system requirements.

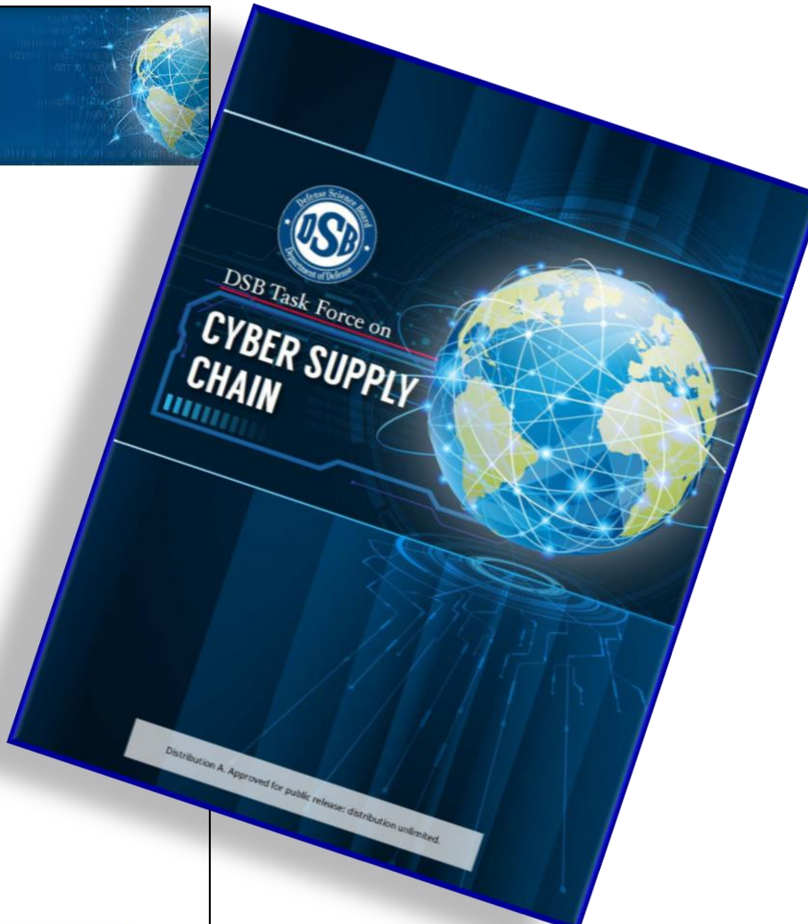
Recommendations from Defense Science Board

Summary of Recommendations

Five categories for improvement

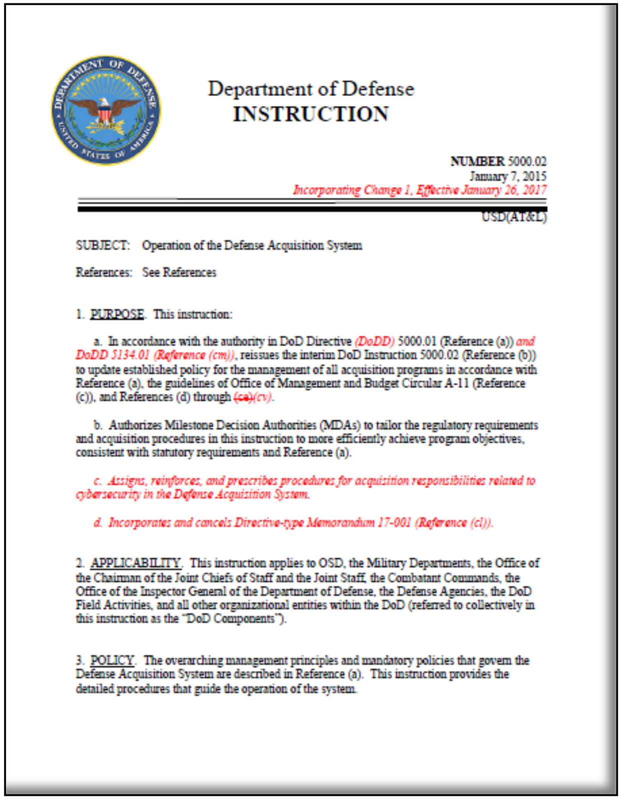
1. Understand supply chain risk
   - Expand vulnerability assessments
2. Mitigate potential vulnerabilities
   - Improve detection and reporting
3. Approach acquisition differently
   - Enhance program protection planning
   - Improve timeliness of supplier vetting
   - Improve system engineering
   - Use JFAC and JAPEC effectively
   - Consider cybersecurity impact of COTS products and components
4. Support life-cycle operations
   - Establish sustainment PPPs for fielded systems
   - Collect and act on parts vulnerabilities
5. Pursue technical solutions

DSB TASK FORCE ON CYBER SUPPLY CHAIN 11



Publicly-released report published Feb 2017
Available at: https://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF

Cybersecurity in Acquisition



Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
Incorporating Change 1, Effective January 26, 2017

USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive *(DoDD)* 5000.01 (Reference (a)) *and DoDD 5134.01 (Reference (cm))*, reissues the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through ~~(ca)~~*(cv)*.

b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

c. Assigns, reinforces, and prescribes procedures for acquisition responsibilities related to cybersecurity in the Defense Acquisition System.

d. Incorporates and cancels Directive-type Memorandum 17-001 (Reference (cl)).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

Acquisition workforce must take responsibility for cybersecurity from the earliest research and technology development through system concept, design, development, test and evaluation, production, fielding, sustainment, and disposal

Scope of program cybersecurity includes:

– Program information Data about acquisition, personnel, planning, requirements, design, test data, and support data for the system.

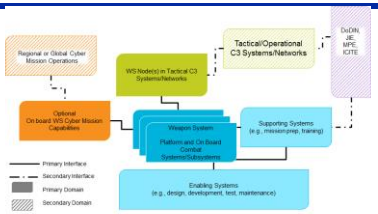
– Organizations and Personnel Government program offices, prime and subcontractors, along with manufacturing, testing, depot, and training organizations

– Networks Government, Government support activities, and contractor owned and operated unclassified and classified networks

– Systems and Supporting Systems The system being acquired, system interfaces, and associated training, testing, manufacturing, logistics, maintenance, and other support systems

Codified in DoDI 5000.02, Enclosure 14, Jan 26, 2017

Design for Cyber Threat Environments



Activities to mitigate cybersecurity risks to the system include:

- **Allocate cybersecurity and related system security requirements to the system architecture and design and assess for vulnerabilities. The system architecture and design will address, at a minimum, how the system:**
  1. Manages access to, and use of the system and system resources.
  2. Is structured to protect and preserve system functions or resources, (e.g., through segmentation, separation, isolation, or partitioning).
  3. Is configured to minimize exposure of vulnerabilities that could impact the mission, including through techniques such as design choice, component choice, security technical implementation guides and patch management in the development environment (including integration and T&E), in production and throughout sustainment.
  4. Monitors, detects and responds to security anomalies.
  5. Maintains priority system functions under adverse conditions; and
  6. Interfaces with DoD Information Network (DoDIN) or other external security services.

DoDI 5000.02, Enclosure 14 establishes a threshold for what to address

Implementation: Engineering Cyber Resilient Workshops

Workshop 1 Findings
1. Requirements derivation is a challenge area
2. Require clarity on Risk Acceptance
3. Assessments should be integrated with and driven by SE Technical Reviews

Workshop 2 Findings/Actions
1. Definitions, Taxonomy & Standards Framework
2. Knowledge Repository
3. Consolidated Risk Guide
4. Assessment Methods
5. Needs Forecasting
6. Industry Outreach

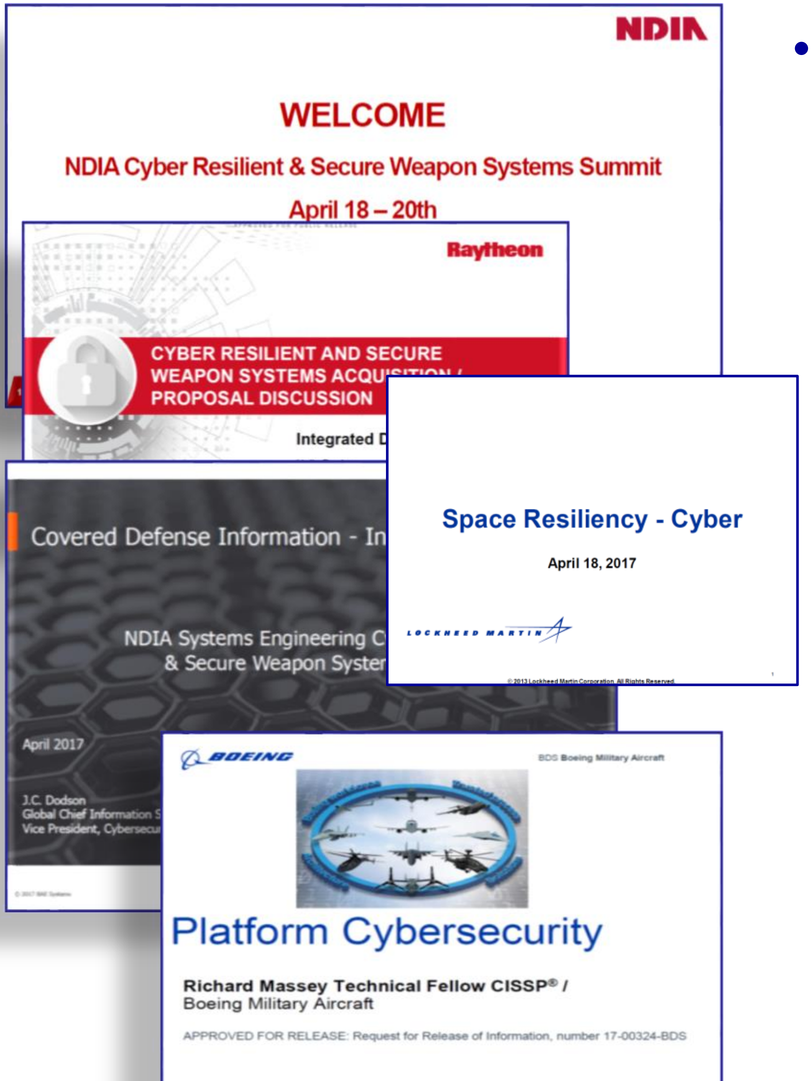
Workshop 3 Findings/Actions
1. Establish DAU CRWS CoP; facilitate definitions, taxonomy standards
2. Develop Risk, Issues, & Opportunities engineering cyber appendix
3. Align assessment approaches
4. Explore S&T opportunities
5. Address Workforce needs
6. Industry Outreach

Workshop 4 (Aug 2017)
Theme: Changing the Culture / Method: Leverage existing engineering approaches

- **Technical Performance Measures and Metrics**
  - Develop Engineering Guidebook
  - Identify TPMs affected by Cyber actions
- **System Engineering Technical Reviews**
  - Validate that existing SETR criteria is sufficient for secure and resilient system design and sustainment
- **Leveraging System Safety**
  - Identify threshold of acceptable risk
  - Quantify the security-driven risk
- **Cyber Resilient Software**
  - Establish an outline to identify engineering design and analysis considerations for the software in secure and resilient weapon systems
- **Risk, Issues, and Opportunity (RIO) Guide**
  - Develop appendix for Cyber Risk

Addressing Recurring Challenges:
Design Guidelines, Implementation, Engineering Assessment

NDIA SE Cyber Resilient Summit and Secure Weapon System Summit
April 18-20, 2017



- **Initial Industry Outreach Aligned with CRWS Series**
  - Industry implementation lessons learned
  - Emphasized need for consistency across communities
  - Discussed approaches to risk acceptance
  - Offered thoughts on implementing safeguards on manufacturing floor
  - Offered areas for improvements to methods, standards, processes, and techniques for cyber resilient & secure weapon systems
  - Thoughts on addressing sustainment challenges

Joint Federated Assurance Center: Software and Hardware Assurance

- **JFAC is a federation of DoD software and hardware assurance (SwA/HwA) capabilities and capacities to:**
  – Provide SW and HW inspection, detection, analysis, risk assessment, and remediation tools and techniques to PM's to mitigate risk of malicious insertion

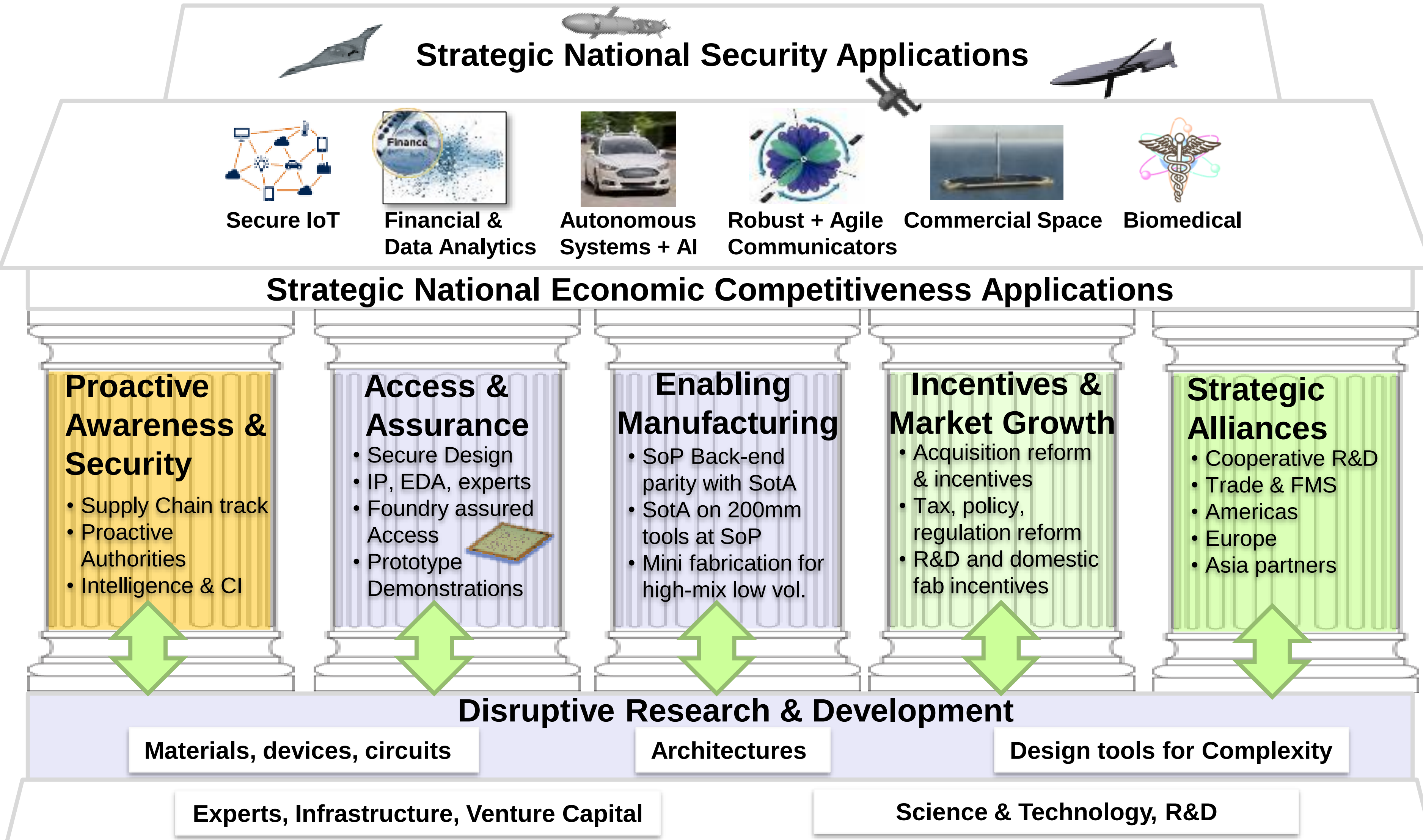
- **JFAC Coordination Center is developing SwA tool and license procurement strategy to provide:**
  – Enterprise license agreements (ELAs) and ELA-like license packages for SwA tools used by all DoD programs and organizations
    - Initiative includes coordinating with NSA's Center for Assured Software to address potential concerns about the security and integrity of the open source products

  – Automated license distribution and management system usable by every engineer in DoD and their direct-support contractors

- **Lead DoD microelectronic hardware assurance capability providers**
  – Naval Surface Warfare Center Crane
  – Army Aviation & Missile Research Development and Engineering Center
  – Air Force Research Lab

Moving Towards Full Operational Capability
JFAC Portal: https://jfac.army.mil/ (CAC-enabled)

US Microelectronics Security and Innovation



These Are Not Cooperative R&D Efforts

U.S. HUMVEE

China's
Dongfeng EQ2050

U.S. Reaper

China's Yìlóng-1

Protecting DoD's Unclassified Information

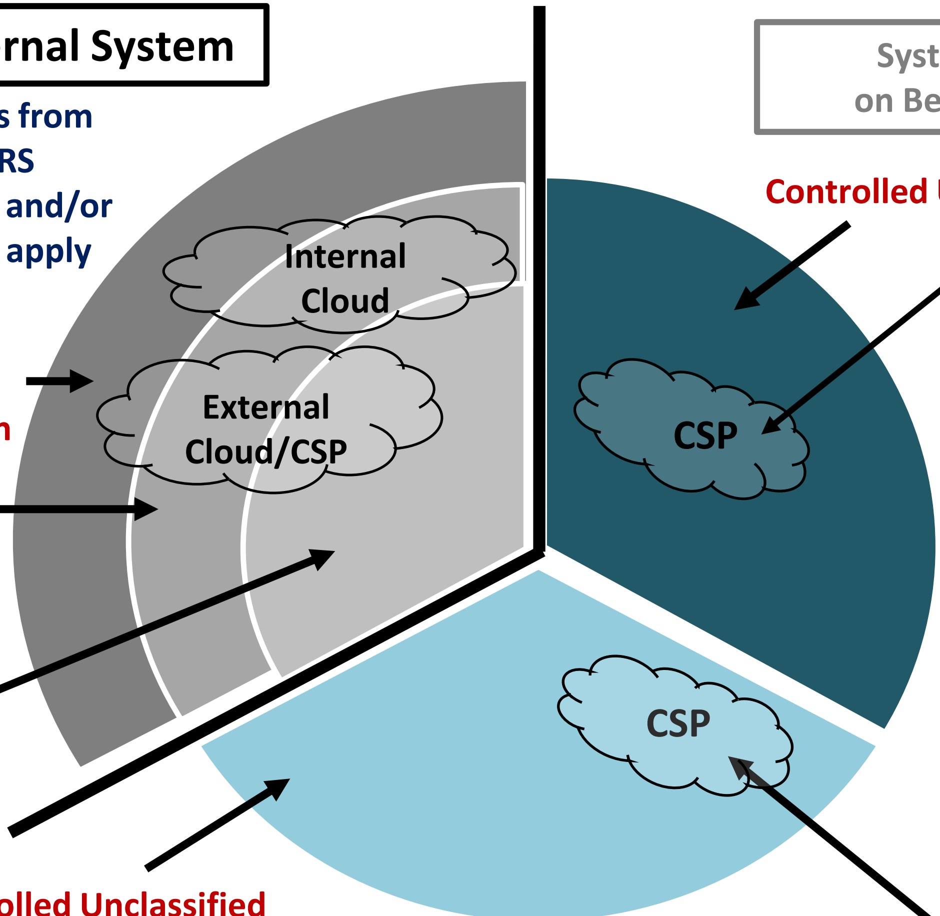
Contractor's Internal System

Security requirements from NIST SP 800-171, DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21 apply

Federal Contract Information

Covered Defense Information (includes Unclassified Controlled Technical Information)

Controlled Unclassified Information



System Operated on Behalf of the DoD

Controlled Unclassified Information

Cloud Service Provider

When cloud services are used to process data on the DoD's behalf, DFARS Clause 252.239-7010 and DoD Cloud Computing SRG apply

DoD Information System

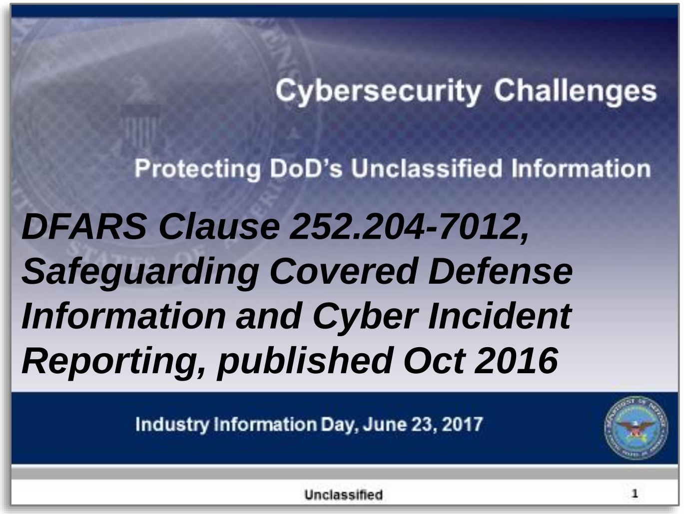
Security requirements from CNSSI 1253, based on NIST SP 800-53, apply

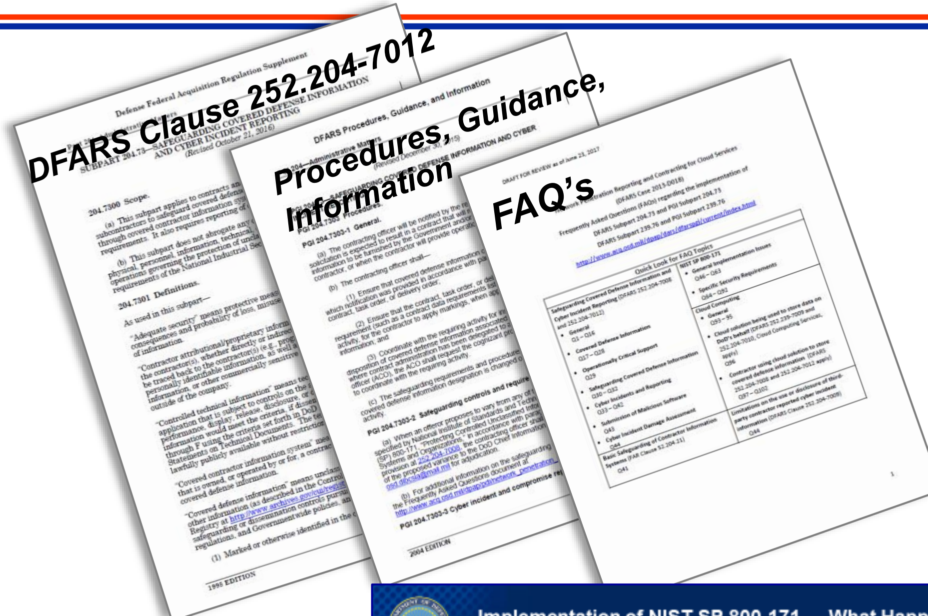
DoD Owned and/or Operated Information System

Cloud Service Provider

When cloud services are provided by DoD, the DoD Cloud Computing SRG applies

Contract Regulation for Safeguarding Covered Defense Information



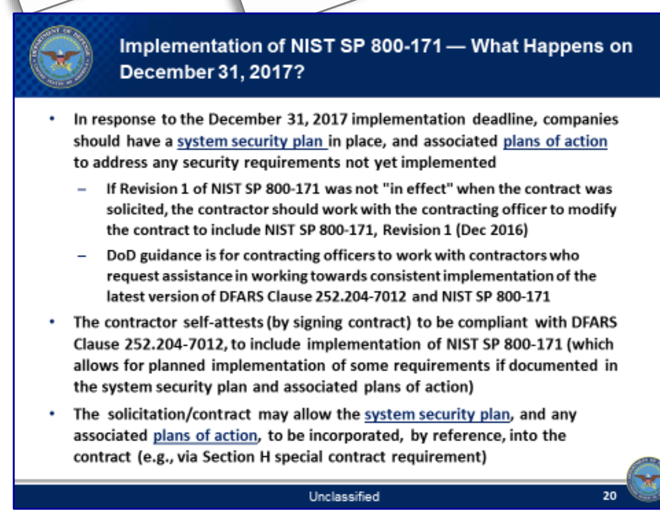


Purpose:

- Establish minimum requirements for contractors and subcontractors to safeguard DoD unclassified covered defense information and report cyber incidents on their contractor owned and operated information systems

Contractor is required to:

- Implement NIST SP 800-171 Controls for unclassified non-Federal Information Systems
- Report cyber incidents affecting covered defense information
- Submit malware when discovered
- Submit media when requested by DoD
- Flow down Clause to subcontractors when covered defense information is on subcontractor networks



Cybersecurity in DoD Acquisition Regulations page:

http://dodprocurementtoolbox.com/ for Related Regulations, Policy, Frequently Asked Questions, and Resources

Cybersecurity for Advanced Manufacturing Systems

Operational Technology Environment

NDIA

ICS systems are long-lived capital investments (15-20 year life)

"Production mindset" with little tolerance for OT down time

Nascent cybersecurity awareness and limited workforce training

Manufacturing jobs bring executable code into system

Technical data flowing through the system is highly valued by adversaries

10 NDIA Cybersecurity for Advanced Manufacturing Joint Working Group April 20, 2017

Challenges in DoD and the Manufacturing Environment are Cross Cutting

Cyber Community of Interest Roadmap Key Capability Areas

Embedded, Mobile, and Tactical Systems (EMT)

Assuring Effective Missions	Assess and control the cyber situation in mission context
Agile Operations	Dynamically reshape cyber systems as conditions/goals change, to escape harm

Resilient Infrastructure	Withstand cyber attacks, and sustain or recover critical functions
Trust	Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error

Cyber Modeling, Simulation, and Experimentation (MSE)

(MSE & EMT) cross-cutting areas in analysis of Joint Chiefs of Staff Cyber Gaps

Program Protection and Cybersecurity in Acquisition Workforce Training

- **ACQ 160: Program Protection Overview**
  - Distance learning (online); ~3 days
  - Provides an overview of program protection concepts, policy and processes, includes overview of DFARS 252.204-7012
  - Intended for the entire Acquisition Workforce, with focus on ENG and PM
  - **Course deployed on DAU website on 15 Aug 2016**

- **ENG 260: Program Protection Practitioner Course (est. deployment Summer 2018)**
  - Hybrid (online and in-class); ~1 week
  - Intended for Systems Engineers and System Security Engineers
  - Focuses on application of program protection concepts and processes, including PM responsibilities for implementing DFARS 252.204-7012

Defense Acquisition University

Effective program protection planning requires qualified, trained personnel

Summary

- **Each system is different; approaches must be tailored to meet the requirement, operational environment and the acquisition**
  - We will embed cybersecurity risk mitigation activities into the acquisition program lifecycle
- **We must bring to bear policy, tools, and expertise to enable cyber resiliency in our systems**
  - Translate IT and network resiliency to weapon system resiliency
  - Establish system security as a fundamental discipline of systems engineering
- **Opportunities for government, industry and academia to engage:**
  - How can we thoughtfully integrate cybersecurity practices in existing standards for embedded software?
  - How can we better integrate program protection and cybersecurity risks into program technical risks?
  - Can we establish system requirements that restricts a system to a set of allowable, and recoverable behaviors?
  - How can we carefully engineer stronger resiliency in systems that are being modernized?

Systems Engineering: Critical to Defense Acquisition










PP/SSE Initiatives Webpage

http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

JFAC Portal

https://jfac.army.mil/ (CAC-enabled)

For Additional Information

Ms. Melinda Reed

ODASD, Systems Engineering

571-372-6562

melinda.k.reed4.civ@mail.mil

Program Protection and Cybersecurity in DoD Policy

DoDI 5000.02 Operation of the Defense Acquisition System

- Assigns and prescribes responsibilities for Cybersecurity, includes security, to the acquisition community
- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD; PM will submit PPP for *Milestone Decision Authority approval* at each Milestone review

DoDI 5200.39 Critical Program Information Identification and Protection Within Research, Development, Test, and Evaluation

- Establishes policy and responsibilities for identification and protection of critical program information
- Protections will, at a minimum, include anti-tamper, exportability features, security, cybersecurity, or equivalent countermeasures.

DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components

DoDI 4140.67 DoD Counterfeit Prevention Policy

- Establishes policy and assigns responsibility to prevent the introduction of counterfeit material at any level of the DoD supply chain

DoDI 8500.01 Cybersecurity

- Establishes the DoD Cybersecurity Program, the DoD Principal Authorizing Official and Senior Information Security Officer to achieve cybersecurity through a defense-in-depth approach that integrates personnel, operations, and technology

The Drive for Innovation in Systems Engineering

D. Scott Lucero

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference

Springfield, VA | October 25, 2017

Defense Research & Engineering Strategy

Mitigate current and anticipated threat capabilities

Enable new or extended capabilities affordably in existing military systems

Create technology surprise through science and engineering

Focus on Technical Excellence

Deliver Technologically Superior Capabilities

Grow and Sustain our S&T and Engineering Capability

Evolving Capability

- **Up until World War II, almost all munitions missed the mark**
  - Massing of forces needed to achieve effects
- **Strategic government investments created an "offset" providing technological advantage**
  - Atomic weapons, precision guided munitions allow reliable targeting
  - Massing of forces no longer absolute necessity
- **Current innovations are driven by industry**
  - Broadly available technology creates a need for velocity

Systems Are Changing

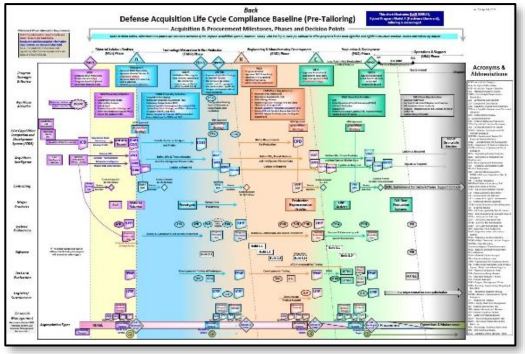
From:	To:
Systems built to last	Systems built to evolve
Heuristic-based decisions	Data-driven decisions
Deeply integrated architectures	Layered, modular architectures
Hierarchical development organizations	Ecosystems of partners, agile teams of teams
Satisfying requirements	Constant experimentation and innovation
Automated systems	Learning systems
Static certification	Dynamic, continuous certification
Standalone systems	Composable sets of mission focused systems

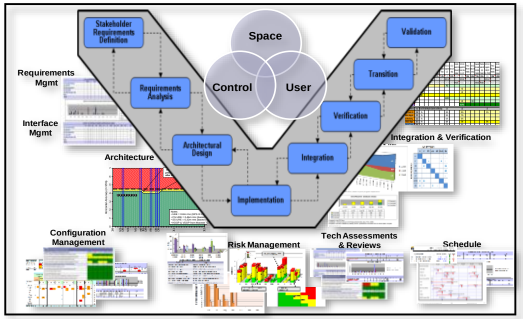
Systems Engineering Needs to Change

Credit: Derived from David Long, Former INCOSE President

Industrial Age Acquisition and Engineering Processes

- **Taylor's scientific management**
  - Empirical methods to synthesize workflows to improve economic efficiency
  - Inspires industrial and systems engineering, business process management, lean six sigma, operations research
- **Optimizing engineering & production drives need for stable requirements, well-defined processes**
- **Optimizing methods to *change* engineering & production requires increasing the cycles of learning:**
  - To identify necessary changes
  - To incorporate those changes into systems

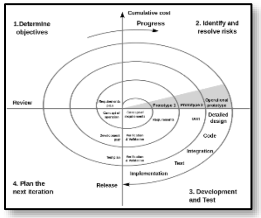




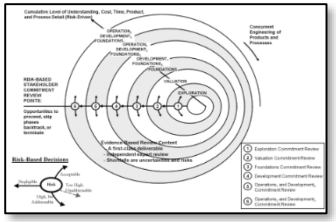
Initiatives to Accelerate Change

- **National Defense Authorization Act (NDAA) for Fiscal Year 2017 Acquisition Agility Act**
  - Modular Open Systems Approaches
  - New authorities for prototyping, experimentation & rapid fielding
  - Defining requirements likely to evolve due to evolving technology, threat or interoperability needs
- **Reorganization of USD(AT&L) – NDAA FY2017**
  - Creates separate organizations for acquisition and for innovative technologies
- **Middle Tier Acquisition Policy – NDAA FY2016**
  - Creates alternate acquisition path for rapid prototyping and fielding
- **Engineered Resilient Systems – 2011**
  - Research and development of deep tradespace analysis methods to address the nature of evolving missions and threats
- **Joint Urgent Operational Needs processes – 2004**

Methods for Managing Software-Intensive Acquisitions

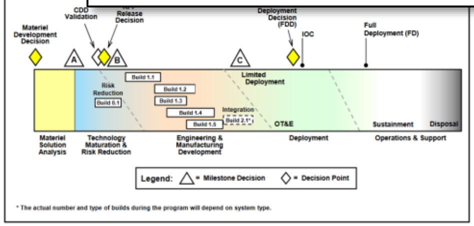


Spiral Development Model (Boehm 1986)

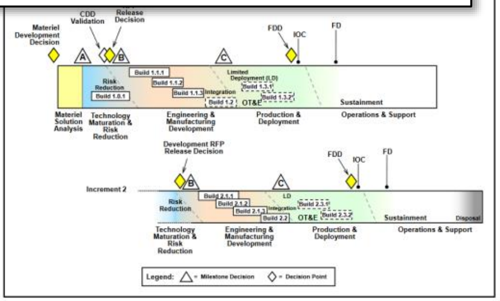


Incremental Commitment Model (Boehm 2007)

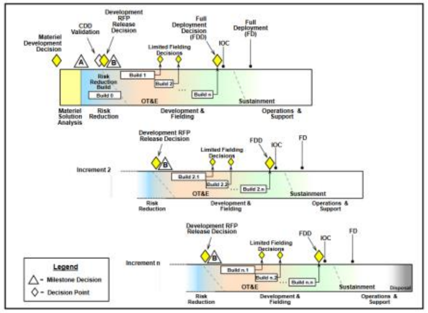
DoD Instruction 5000.02 – Operation of the Defense Acquisition System (Jan 2015)



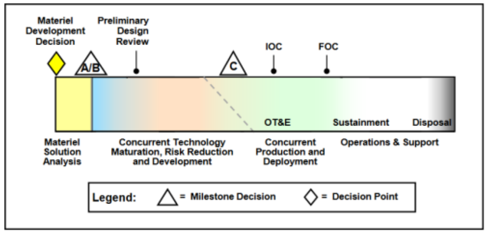
Software Intensive



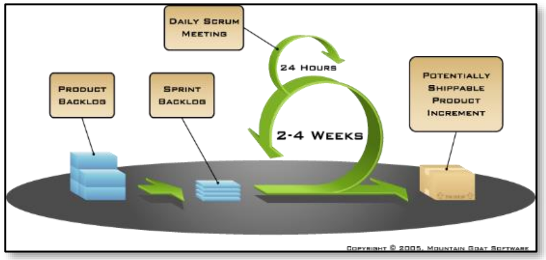
Hybrid – Software Dominant



Incrementally Deployed Software Intensive



Accelerated



Agile Development – 2001

Other Systems Engineering Perspectives

- **MIL-STD-499 Engineering Management**
  - Issued by Air Force in 1969 and 1974
    - Draft MIL-STD-499B never published in 1990's acquisition reform era
  - Not time-sequenced, like the V-model
  - Process seems to encourage trades in the "need-space" and the "solution-space"
  - Less focused on production
  - Less prescriptive – less useful in organizing activities

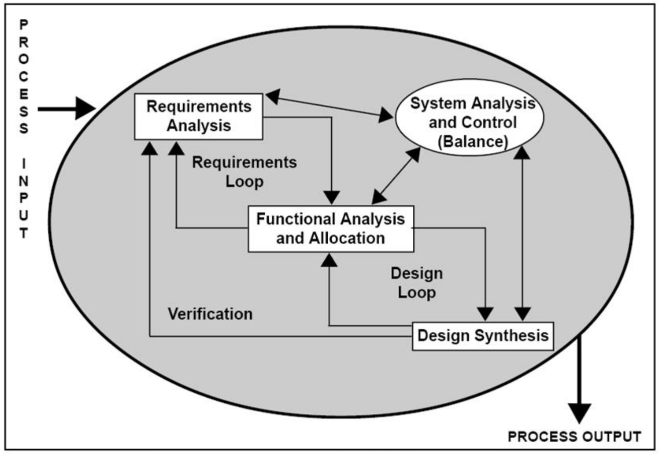
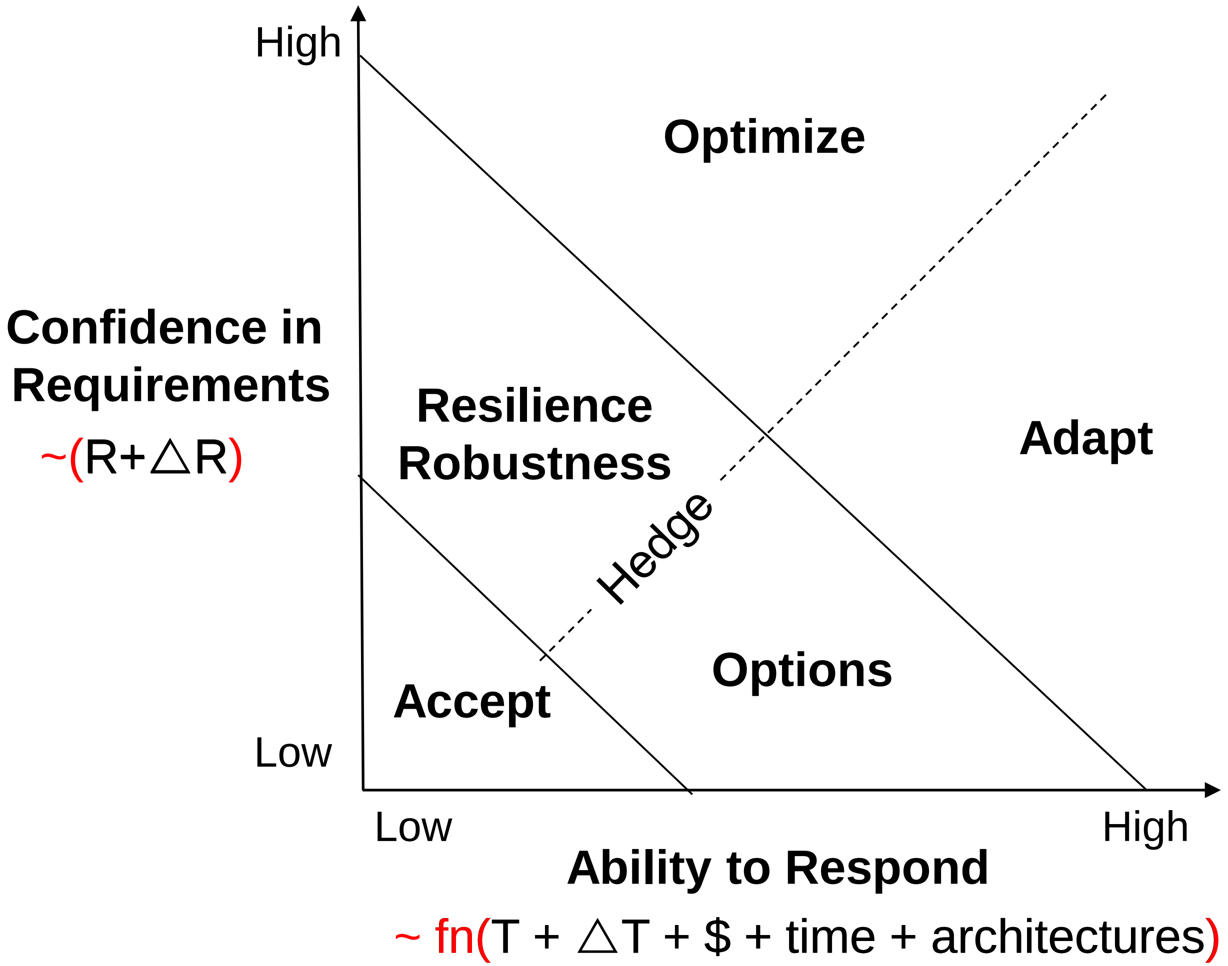


Figure 1-3. The Systems Engineering Process

Methods for Selecting Acquisition Approaches



Notes:

- Framework helps overcome tendency to develop optimal solutions to static requirements
- Each axis belongs to a separate community
- Uncertainty around Requirements and Technology can be informed by intelligence community

Credit: Derived from Michael Pennock, Stevens Institute

Interesting Research Questions

- **Gauging confidence in requirements, ability to respond**
- **Analysis of trades across the mission space and the solution space**
- **Gauging risk, rework**
- **Hedging methods**
- **Actual increases in velocity of capability delivered**
- **Methods to increase ability to respond**
  - e.g., MBSE, advanced manufacturing
- **Dynamic and continuous learning and certification**
- **Multiple systems interrelationships**
  - Portfolio management, mission engineering
- **Others?**

For Additional Information

D. Scott Lucero

Deputy Director, Strategic Initiatives

Office of the DASD

Systems Engineering

571-372-6452 | don.s.lucero.civ@mail.mil

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

Modeling the Digital System Model (DSM) Data Taxonomy

Philomena Zimmerman

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference

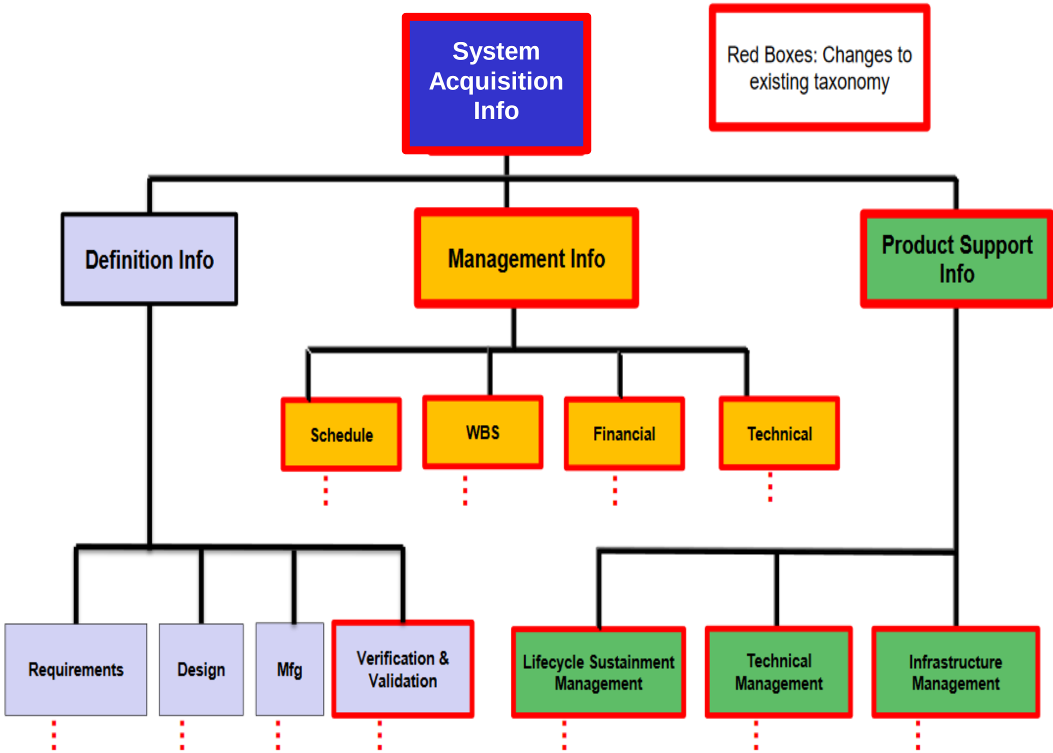
Springfield, VA | October 25, 2017

Agenda

- DSM Data Taxonomy Overview
- Evolution of the DSM Data Taxonomy (Tabular, Mind Map, SysML)
- Modeling the DSM Data Taxonomy
- Benefits
- Path Forward

DSM Data Taxonomy Overview

- **Purpose**
  - Provides a model to aid programs in defining an authoritative source of truth
  - Builds an integrated taxonomy providing stakeholders an organized structure for the types of technical data to be considered across the life cycle
  - Establishes a Common Vocabulary that can be used by all programs



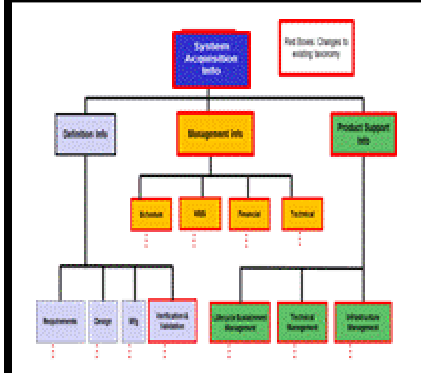
A change from document centric taxonomy in DAG CH 3–4.1.7 Technical Data Management Process.

Use as a basis to drive the community towards Digital Engineering across disciplines, systems and enterprises to support life cycle activities from concept to disposal.

DSM Intended Use

Defines the broad categories of data

DSM Data Taxonomy



Component of the DE Infrastructure

Provides the program's DE ecosystem

DE Ecosystem

Identifies the data and data rights

Document Views

Provides multiple views to support ***decisions***

Data Views

Acquisition Views

Other Views

DSM Data Taxonomy provides the broad categories of data that should be considered across the lifecycle

Data Taxonomy Uses

- The taxonomy serves as a common vocabulary for enterprise and program consideration.
- Use it to define the data the program will need to create and manage.
- Use it to determine what tools will use or produce the data.
- Use it to determine who owns and controls the data at any point in time in a programs life.
- Use it to identify what data will be delivered on contract, what format the data should be received in.
- Use it to identify what data has associated data restrictions.
- Use it to identify what data needs to be protected and handled.
- Use it to define the data that belongs in views, digital and or other artifacts.

Evolution to Modeling the DSM Data Taxonomy

Tabular Tool

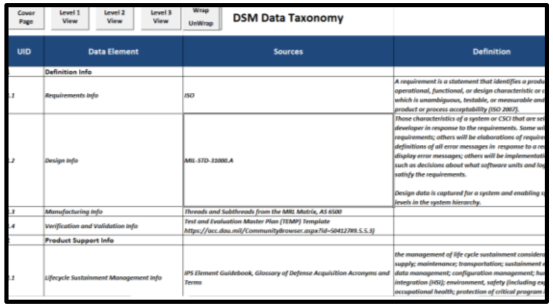
- Initial attempt to organize and construct a hierarchical structure for technical data in a system from documents and guidelines (e.g., DAG, ICD, CDD, SEP, TEMP, MIL-STD, SME, etc.)

Mind Mapping Tool

- Prototype testing using a mind mapping tool to visualize hierarchical relationships between system components and their respective digital artifacts

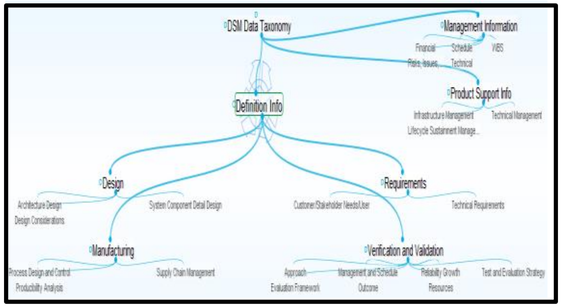
SysML Modeling Tool

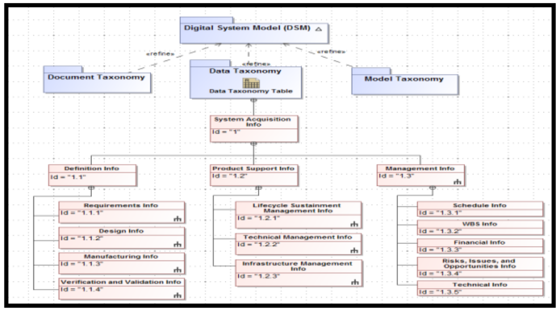
- Utilized a System Modeling Language (SysML) modeling tool to construct a hierarchical structure and enable the capture of digital technical data for use and reuse in a model


Cover Page | Level 1 View | Level 2 View | Level 3 View | Wrap UnWrap

DSM Data Taxonomy

UID	Data Element	Sources	Definition
[illegible]	Definition Info		
.1	Requirements Info	ISO	A requirement is a statement that identifies a produ[…] operational, functional, or design characteristic or c[…] which is unambiguous, testable, or measurable and[…] product or process acceptability (ISO 2007).
.2	Design Info	MIL-STD-31000.A	Those characteristics of a system or CSCI that are se[…] developer in response to the requirements. Some wi[…] requirements; others will be elaborations of require[…] definitions of all error messages in response to a re[…] display error messages; others will be implementati[…] such as decisions about what software units and log[…] satisfy the requirements. Design data is captured for a system and enabling s[…] levels in the system hierarchy.
.3	Manufacturing Info	Threads and Subthreads from the MRL Matrix, AS 6500	
.4	Verification and Validation Info	Test and Evaluation Master Plan (TEMP) Template https://acc.dau.mil/CommunityBrowser.aspx?id=504127#9.5.5.3)	
[illegible]	Product Support Info		
.1	Lifecycle Sustainment Management Info	IPS Element Guidebook, Glossary of Defense Acquisition Acronyms and Terms	the management of life cycle sustainment considera[…] supply; maintenance; transportation; sustainment e[…] data management; configuration management; hu[…] integration (HSI); environment, safety (including ex[…] occupational health; protection of critical program i[…]





DSM Data Taxonomy in Excel

Cover Page | Level 1 View | Level 2 View | Level 3 View | Level All View | Wrap | UnWrap

DSM Data Taxonomy

UID	Data Element	Sources
1	Definition Info	
2	Product Support Info	
3	Management Info	

Cover Page | Level 1 View | Level 2 View | Level 3 View | Level All View | Wrap | UnWrap

DSM Data Taxonomy

UID	Data Element	Sources	Definition	Comments
1	Definition Info			
1.1	*Requirements Info*	*ISO*	*A requirement is a statement that identifies a product or processes operational, functional, or d*	
1.2	*Design Info*	*MIL-STD-31000A*	*Those characteristics of a system or CSCI that are selected by the developer in response to the re*	

Cover Page | Level 1 View | Level 2 View | Level 3 View | Level All View | Wrap | UnWrap

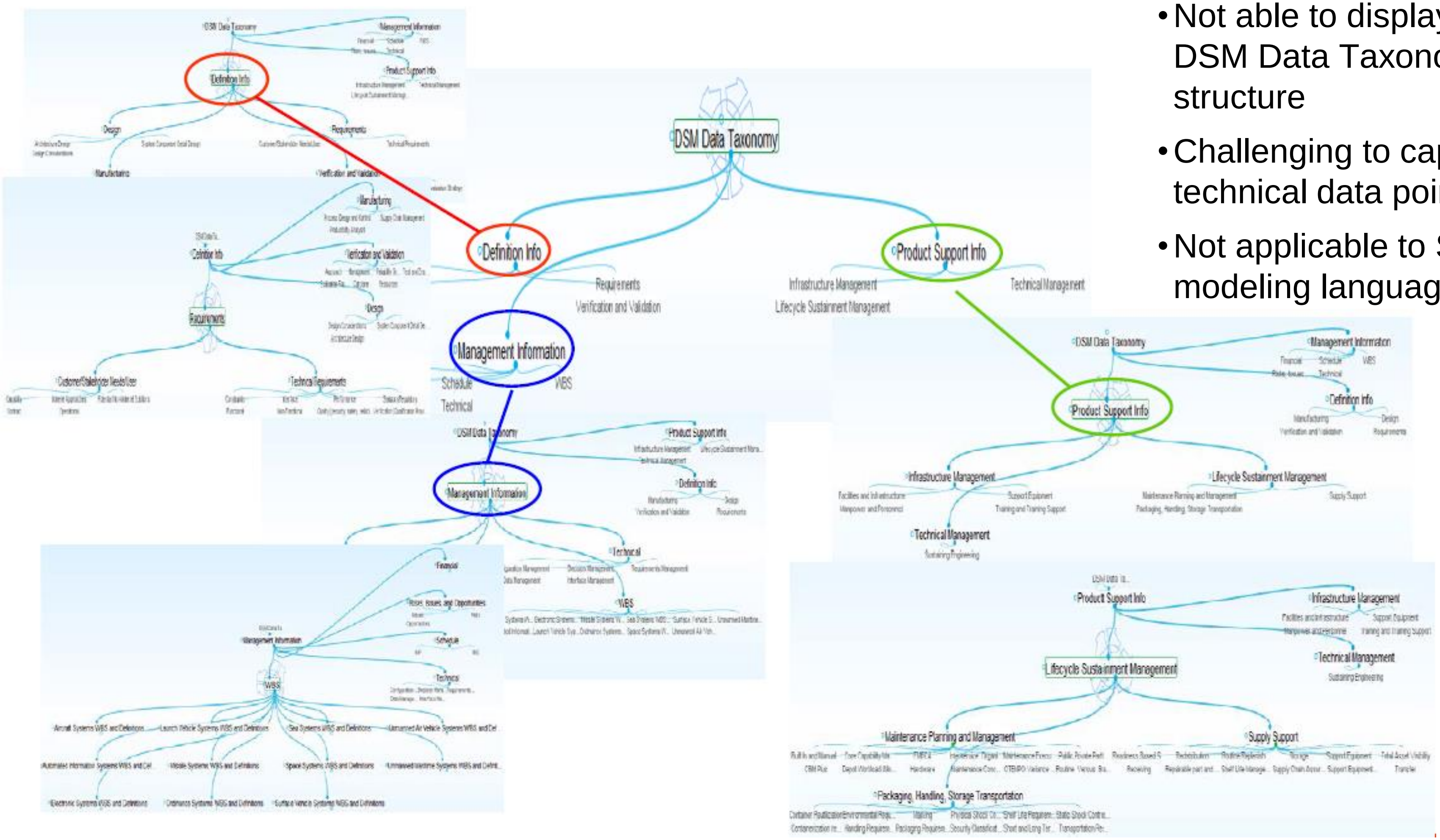
DSM Data Taxonomy

UID	Data Element	Sources	Definition	Comments
1	**Definition Info**			
1.1	***Requirements Info***	***ISO***	***A requirement is a statement that identifies a product or processes operational, functional, or design***	
1.1.1	Customer/Stakeholder Needs/User Info	DI-IPSC-81431A/SEBOK	Set of stakeholder requirements are clarified and translated from statements of need into engineerir	
1.1.1.1	Capability	ICD	A capability is the ability to achieve a desired effect under specified standards and conditions throu	
1.1.1.1.1	Capability Gap	ICD	The inability to execute a specified course of action. The gap may be the result of no existing capabi	
1.1.1.1.2	Required Capabilities	ICD	A capability required to meet an organization's roles, functions, and missions in current or future op	
1.1.1.1.3	Enabling Capabilities	DoDD 3700.01	services, systems, processes, and related infrastructure that enable the exercise of authority and di	
1.1.1.1.4	Applicable Joint Capability Areas (JCAs)	ICD	JCAs are collections of similar capabilities logically grouped to support strategic investment decisic	
1.1.1.2	Contract	DI-IPSC-81431A/SEBOK		
1.1.1.3	Operational	DI-IPSC-81431A/SEBOK		
1.1.1.3.1	Mission Information	JCIDS products (FAA, FNA, FSA); ICD, CDD, OMS/MP)		
1.1.1.3.1.1	Mission Essential Tasks	Requirements documents (Operational and Functional Concepts; JCIDS pr	A collective task a unit must be able to perform successfully in order to accomplish its doctrinal or	
1.1.1.3.1.2	Mission Objectives/Operational Outcomes/Effects/Military Objective Achieved Info	Requirements documents (Operational and Functional Concepts; JCIDS pr	Effectiveness The overall degree of mission accomplishment by a system under realistic conditions (	
1.1.1.3.1.2.1	Concept of Operations Summary	ICD	A verbal or graphic statement, in broad outline, of a commander's assumptions or intent in	
1.1.1.3.1.2.2	Operational Outcome	ICD	(d) Identify what measurable operational outcomes are required; what effects must be produced to	
1.1.1.3.1.3	Measures of Effectiveness (MoE)	CDD	Measures designed to correspond to accomplishment of mission objectives and achievement	
1.1.1.3.1.4	Measures of Suitability (MoS)	CDD	Measure of an item's ability to be supported in its intended operational environment. MOS's typical	
1.1.1.3.2	Threat and Operational Environment Info	System Threat Assessment Report (STAR)		
1.1.1.3.2.1	Operational Environment	System Threat Assessment Report (STAR)	This is a composite of conditions, circumstances, and influences that affect employment of military	
1.1.1.3.2.2	Threat Summary	System Threat Assessment Report (STAR)	The sum of the potential strengths, capabilities, and strategic objectives of any adversary that can li	
1.1.1.3.3	Tasks	Functional Area Analysis (FAA); Functional Needs Assessment (FNA); Oper	A clearly defined and measurable activity accomplished by individuals and organizations. (FM 7-0)	
1.1.1.3.3.1	Conditions	Formation OMS/MP (Collective Tasks, Conditions, Standards); System OM	Those variables of an operational environment or situation in which a unit, system, or individual is	
1.1.1.3.3.2	Standards	Formation OMS (Collective Tasks, Conditions, Standards); System OMS (S	A quantitative or qualitative measure and criterion for specifying the levels of performance of a tas	
1.1.1.3.3.3	Measures of Performance (MoP)	Formation OMS (Collective Tasks, Conditions, Standards); System OMS (S	A criterion used to assess friendly actions that are tied to measuring task accomplishment. (JP 3-0)	
1.1.1.3.4	Timeframe and Justification	Required Capabilities (RC) (published by ARCIC and/or COEs); Army Warf	The timeframe considered in the CBA is important both to help establish the conditions and threats	
1.1.1.3.5	Defense Planning Scenarios	DI-IPSC-81431A/SEBOK	This is a graphic and narrative description of area, environment, means (political, economic, social,	
1.1.1.3.6	Using Organization(s) (supported SoS)	Basis of Issue (BOI) Guidance		
1.1.1.3.6.1	Quantities issued per using organization	Basis of Issue (BOI) Guidance		
1.1.1.3.7	Critical Operational Issues and Criteria (COICs)	Test and Evaluation Master Plan (TEMP)		
1.1.1.4	Potential Non-Materiel Solutions	ICD	These are changes in doctrine, organization, training, materiel, leadership and education, personne	
1.1.1.5	Materiel Approaches	ICD	Correction of a deficiency, satisfaction of a capability gap, or incorporation of new technology that	

Challenges

- Extensive and complex view (The Excel file expands to over 400 line items)
- Difficulty discerning hierarchical relationship between data elements
- Very manual process to render diagrams and show relationships between elements.
- Cumbersome to track changes

DSM Data Taxonomy in The Brain Mind Mapping Tool

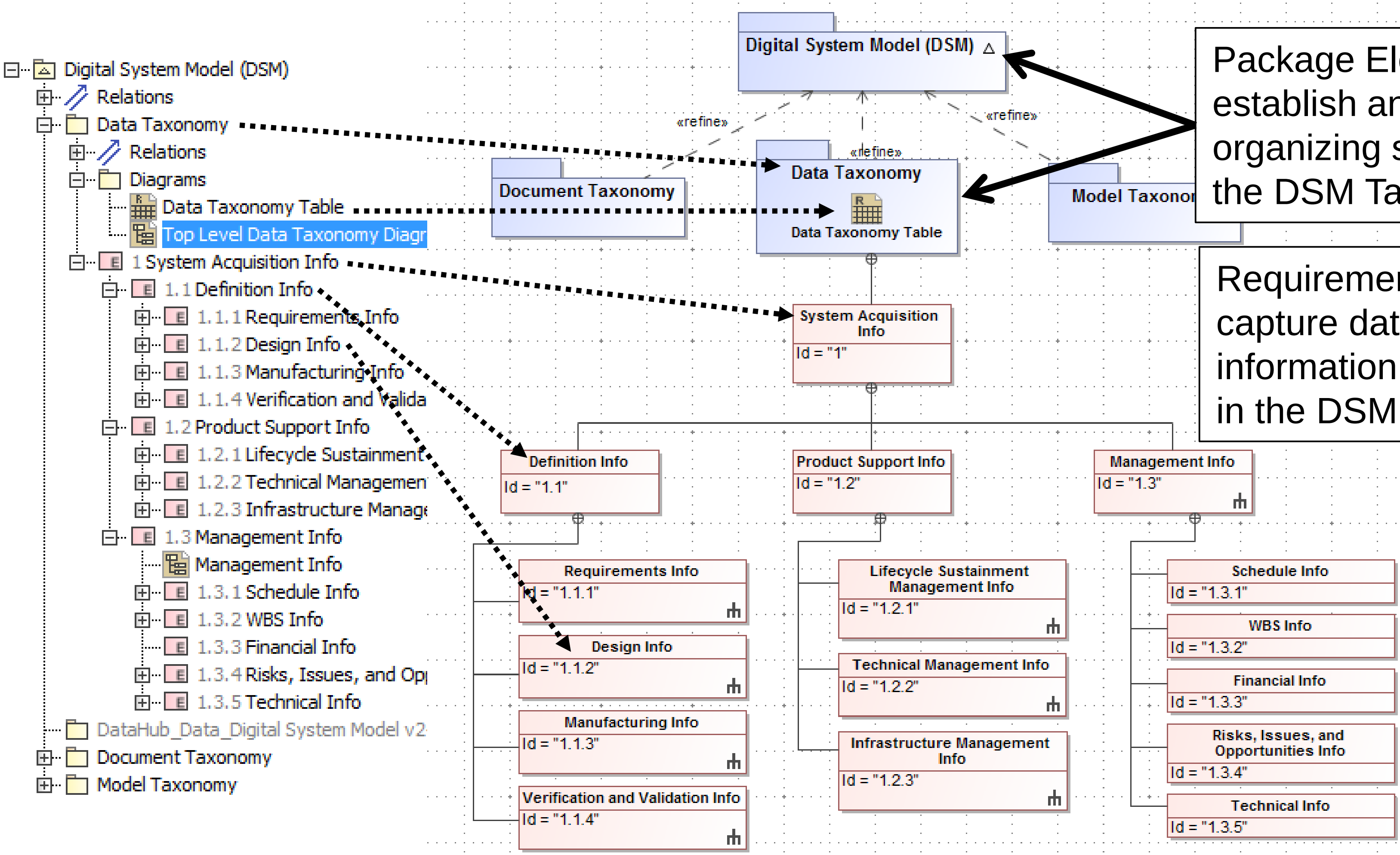


Challenges

- Not able to display the entire DSM Data Taxonomy structure
- Challenging to capture technical data points
- Not applicable to SysML modeling language

Modeling the DSM Data Taxonomy

- **The model is used to create a hierarchy diagram view.**



Package Elements establish an initial organizing structure for the DSM Taxonomy.

Requirement elements capture data within information categories in the DSM Taxonomy.

Modeling the DSM Data Taxonomy (cont.)

- **The model is used to create a table View.**

#	△ Id	Name	Source	Text
1	1	System Acquisition Info		This taxonomy represents current knowledge about data classes and data types captured in todays defense acquisition systems programs. This taxonomy was built as an organizing construct that could be used by programs as an aid to managing their data and defining viewpoints that would need to be auto generated from the Digital System Model.
2	1.1	Definition Info	ISO	A requirement is a statement that identifies a product or processes operational, functional, or design characteristic or constraint, which is unambiguous, testable, or measurable and necessary for product or process acceptability (ISO 2007).
3	1.1.1	Requirements Info	ISO	A requirement is a statement that identifies a product or processes operational, functional, or design characteristic or constraint, which is unambiguous, testable, or measurable and necessary for product or process acceptability (ISO 2007).
4	1.1.1.4	Customer/Stakeholder Ne	DI-IPSC-81431A/S	Set of stakeholder requirements are clarified and translated from statements of need into engineering-oriented language in order to enable proper architecture definition, design, and verification activities that are needed as the basis for system requirements analysis. Stakeholder needs and requirements represent the views of those at the business or enterprise operations level—that is, of users, acquirers, customers, and other stakeholders as they relate to the problem (or opportunity), as a set of requirements for a solution that can provide the services needed by the stakeholders in a defined environment. Using enterprise-level life cycle concepts (see Business or Mission Analysis for details) as guidance, stakeholders are led through a structured process to elicit stakeholder needs (in the form of a refined set of system-level life-cycle concepts). Stakeholder needs are transformed into a defined set of Stakeholder Requirements, which may be documented in the form of a model, a document containing textual requirement statements or both.
5	1.1.1.4.4	Capability	ICD	A capability is the ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. (TRADOC Regulation 71-20)
6	1.1.1.4.4.4	Capability Gap	ICD	The inability to execute a specified course of action. The gap may be the result of no existing capability, lack of proficiency or sufficiency in an existing capability solution, or the need to replace an existing capability solution to prevent a future gap. See CJCSI 3170.01

Modeling the DSM Data Taxonomy (Data Field Descriptions)

- **"#" is the number of the data element.**
- **"ID" indicates the hierarchical location of the data element in the Data Taxonomy.**
- **"Name" provides a unique name for each data element in the Data Taxonomy.**
- **"Source" provides one or more references that were used to derive the data element.**
- **"Text" provides a definition for each data element. Use this column to understand what data to captured for each of the associated data elements.**

Benefits to Modeling the DSM Data Taxonomy

- **Manage Complexity**
  - Provides a method to use and navigate the DSM Data Taxonomy
  - Manages hierarchical data structure
- **Preserve and Enable Reuse of Heritage Knowledge**
  - Provides a method to capture, store, and use/reuse data
  - Offers accessible, shareable, and transparent data for current and future workforce
- **Outline Data Structure**
  - Provide an organized structure for the types of program data that should be considered across the life cycle

Path Forward

- **Content Validation of DSM Data Taxonomy**
  - Work with Services to review and provide comment on the DSM Data Taxonomy
  - Incorporate into INCOSE Digital Artifact Challenge
- **Finalize and deploy DSM Data Taxonomy for Usage after Reviews and Revisions**
- **Model Document and Model Taxonomies**
- **Manage Changes**

Systems Engineering: Critical to Defense Acquisition

Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Philomena Zimmerman

ODASD, Systems Engineering

571-372-6695 | philomena.m.zimmerman.civ@mail.mil

Other Contributors:

Frank Salvatore

973-265-9837 | frank.j.salvatore.ctr@mail.mil

Tracee Walker Gilbert, Ph.D.

571-372-6145 | tracee.w.gilbert.ctr@mail.mil

Tyesia Pompey Alexander, Ph.D.

571-372-6697 | tyesia.p.alexander.ctr@mail.mil

Allen Wong

571-372-6788 | allen.wong4.ctr@mail.mil

DoD Joint Federated Assurance Center (JFAC) 2017 Update

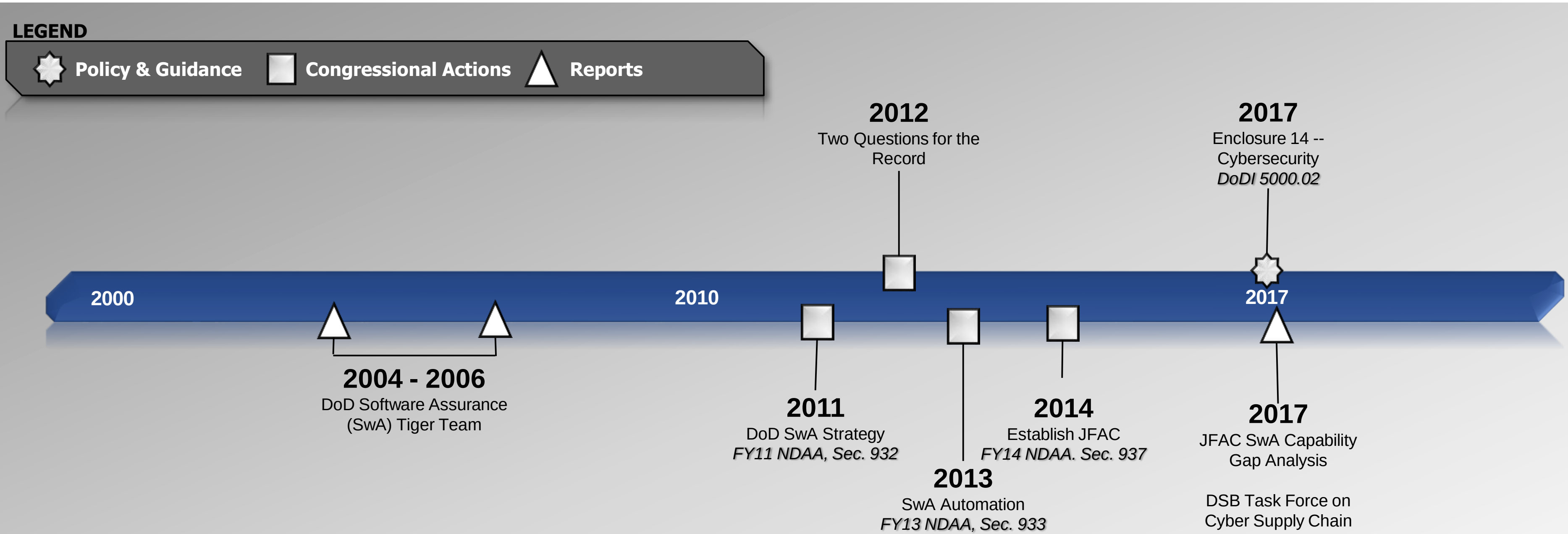
Thomas Hurt

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference

Springfield, VA | October 26, 2017

How Did We Get Here?



Congress and DoD have acknowledged the need for increased software assurance to improve confidence in secure and resilient weapon systems for over a decade.

JFAC: Joint Federated Assurance Center

Joint Federated Assurance Center (JFAC)

FY14 NDAA Section 937—Joint Federated Assurance Center (JFAC)

Key provisions:

- “provide for the establishment of a **joint federation of capabilities** to support the trusted defense system needs…to ensure security in the **software** and **hardware** developed, acquired, maintained, and used by the Department”
- “consider whether capabilities can be met by existing centers”
- **“[if gaps] shall devise a strategy [for] resources [to fill such gaps]”**
- “[NLT 180 days, SECDEF shall] issue a **charter**…”
- “submit to congressional defense committees…a **report** on funding and management”

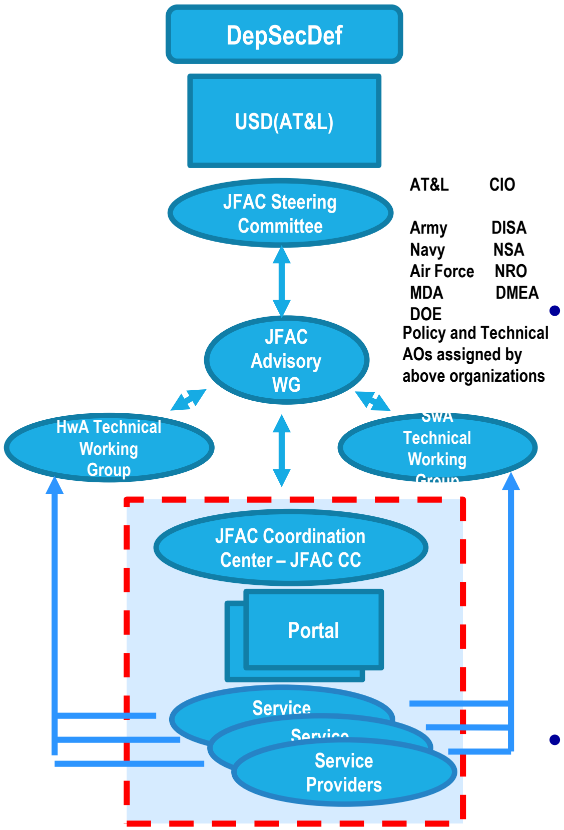
Charter elements:

- Role of federation in supporting program offices
- SwA and HwA expertise and capabilities of the Federation, including policies, standards, requirements, best practices contracting, training and testing
- R&D program to improve code vulnerability analysis and testing tools
- Requirements to procure manage, and distribute enterprise licenses for analysis tools

What Has DoD Done?

- **Development of Concept of Operations (CONOPs) and Charter**
- **Establishment of JFAC Coordination Center (JFAC-CC), Steering Committees, Working Groups (WGs)**
- **Piloting Software Assurance (SwA) license distribution and management**
- **Conduct SwA and Hardware Assurance (HwA) Capability Gap Analysis**

JFAC Operational Structure



- **SwA and HwA Working Groups**
  - Collaboration and shared prioritization in daily/weekly activities, meet on a regular basis
  - Recommend policy and guidance
  - Provide community forum for “hard problem” analysis and question/answer
- **JFAC Coordination Center**
  - Coordination of **Service Providers**
  - Supports programs with situational awareness, information/best practices, coordination
  - SwA analysis tool license distribution
  - **Portal:** https://jfac.army.mil
  - Assessment Knowledge Base (future)
- **JFAC Action Officer (AO) WG**
  - AOs for JFAC Steering Committee
  - Maintain enterprise and strategy cognizance
  - Reporting and ROI status

What's Going On Now?

- JFAC Web portal and SwA tool license distribution
- Security Classification Guide
- Field Programmable Gate Array (FPGA) Strategy
- Resourcing

What's Next?

- **Develop JFAC Full Operational Capability (FOC) strategy**
  - Improve DoD SwA throughout Lifecycle Planning, Execution and Sustainment
  - Invest in Technology and Resources
  - Upgraded Infrastructure for Federated DoD-wide Coordination of Software Assurance
  - Linking Sustainment to Early Program Development

- **JFAC website on SIPR, JWICS**
  - One-stop shop for SwA tools and best practices
  - New S&T and Assessment Knowledge Base portals
  - https://jfac.army.mil

Conclusion

- **The JFAC's goal is to provide DoD programs a one-stop shop to request, evaluate, and obtain resources to improve their software assurance practice.**
  - SwA analysis tool license distribution and management
  - Service providers for programs' SwA work; SMEs focused on hard problems
  - SwA best practices

- **JFAC is addressing key software assurance gaps.**
  - Developing FOC strategy to execute as resourcing becomes available
  - Publishing best practices at JFAC web portal (https://jfac.army.mil)

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Mr. Thomas Hurt

ODASD, Systems Engineering

571-372-6129

thomas.d.hurt.civ@mail.mil

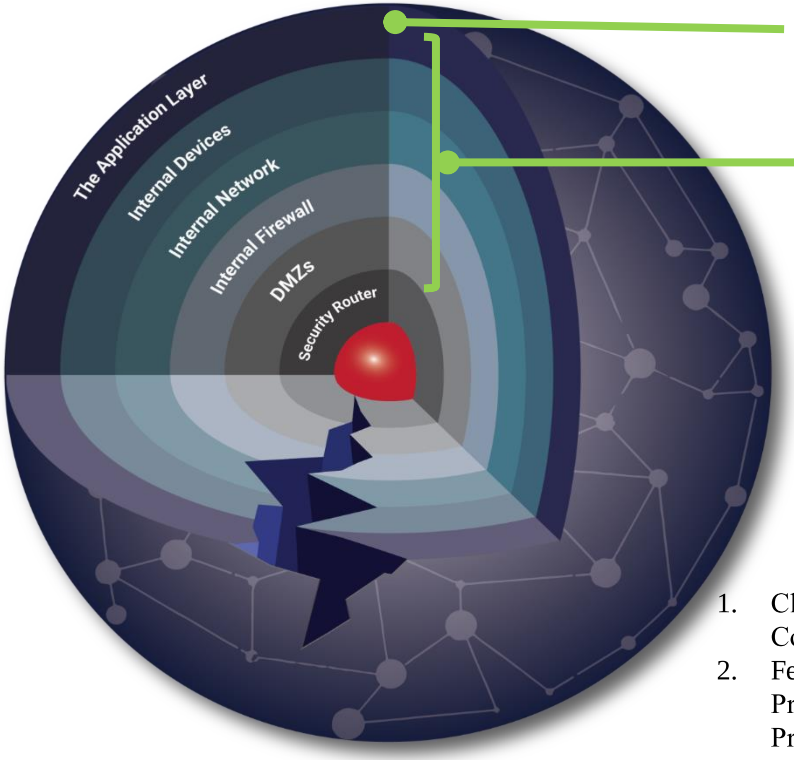
Achieving DoD Software Assurance (SwA)

Thomas Hurt
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 26, 2017

First Line of Defense in Software Assurance Is the Application (Software) Layer

Software assurance (SwA) provides the required level of confidence that software functions as intended (and only as intended) and is free of (known) vulnerabilities, either intentionally or unintentionally designed or inserted in software, throughout the life cycle.

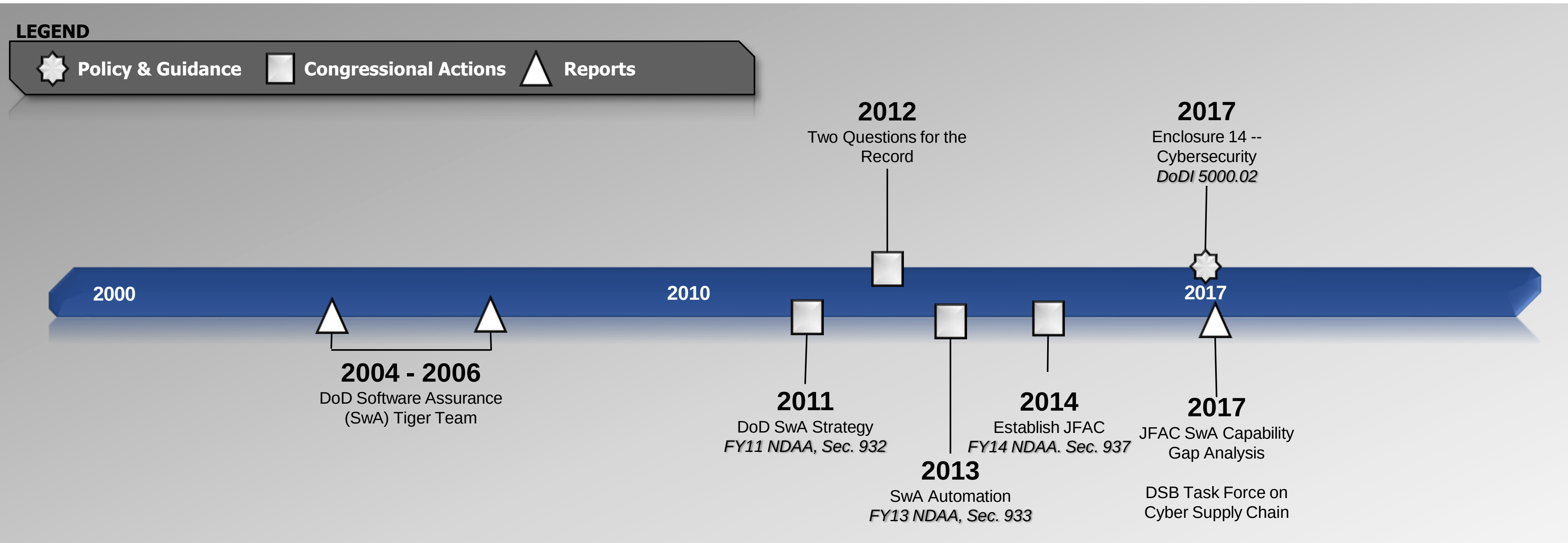


84% of breaches exploit vulnerabilities in the application[1]

Yet funding for IT defense vs. software assurance is 23 to 1[2]

1. Clark, Tim, "Most Cyber Attacks Occur from This Common Vulnerability," *Forbes*, 03-10-2015
2. Feiman, Joseph, "Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves," *Gartner*, 09-25-2014. G00269825

How Did We Get Here?

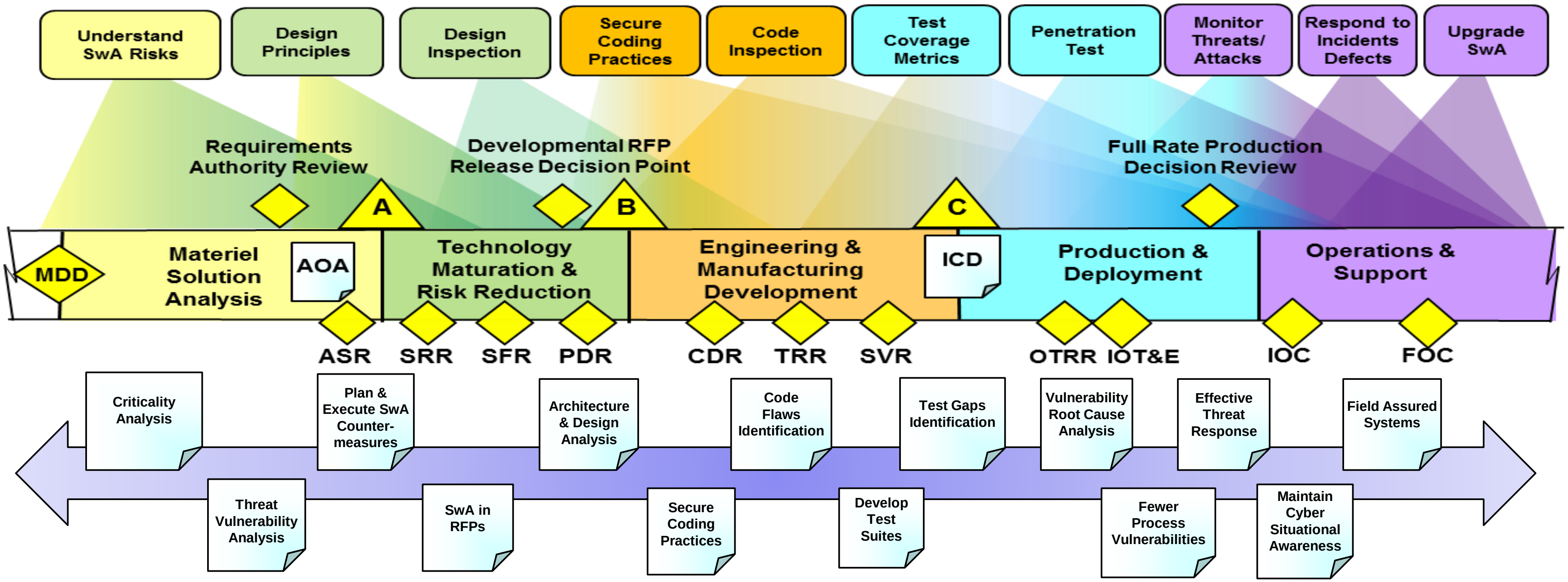


Congress and DoD have acknowledged the need for increased software assurance to improve confidence in secure and resilient weapon systems for over a decade.

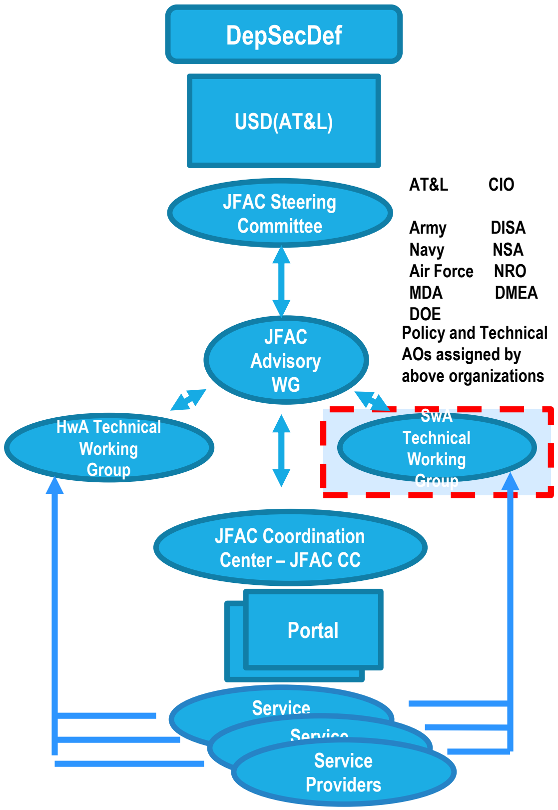
JFAC: Joint Federated Assurance Center

How to Engineer Software Assurance Across the DoD Acquisition Life Cycle

Software Assurance best practices, as a part of Systems Engineering, focus on increasing the level of confidence of software functioning as intended.



SwA within DoD



- **JFAC SwA Working Group**
  - Collaboration and shared prioritization in daily/weekly activities, meet on a regular basis
  - Recommend SwA policy and guidance
  - Provide community forum for “hard problem” analysis and question/answer

- **DoD SwA Community of Practice**
  - Tri-leads; meets quarterly with various DoD stakeholders’ participation
  - Sponsors research and pilots into hard SwA problems

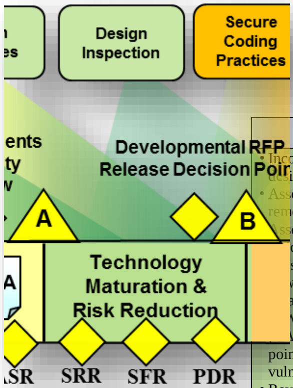
What's Going on Now? (1 of 3)

- **DoD Software Assurance Community of Practice**
  - Past products include: Contract language for integrating SwA; State-of-the-Art Resource (SOAR) for SW Vulnerability Detection, Test, and Evaluation; SwA metrics
  - Recent Topics and Ongoing Activities
    - SwA Risk Assessment process
    - Malware discovery in binary code
    - SwA analysis of mobile software

- **The Journal of Cyber Security and Information Systems: Design & Development Process for Assured Software–Vol 1***
  - Software Assurance in the Agile Software Development Lifecycle
  - Is Our Software REALLY Secure?
  - Development and Transition of the SEI Software Assurance Curriculum
  - Keys to Successful DoD Software Project Execution
  - Hacker 101 & Secure Coding: A Grassroots Movement toward Software Assurance

* https://www.csiac.org/journal-issue/design-and-development-process-for-assured-software-volume-1/

What's Going on Now? (2 of 3)



Acquisition Phase Considerations

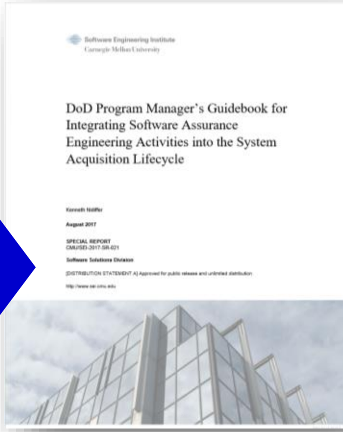
SOFTWARE ASSURANCE CONSIDERATIONS (TMRR Phase)

- Incorporate SwA requirements, tool use, metrics, and assurance thresholds into solicitations. Architectures, designs, and code developed for prototyping are frequently reused later in development.
- Assess system functional requirements and verification methods for inclusion of SwA tools remediation across the development life cycle.
- Assess requirements for SwA are correct and complete regarding assurance. Consider mea ders and adversaries using malicious inserts; system characteristics; interoperability wi sion threads; and other factors. Assure that mapping and traceability are maintained as wnstream assessments.
- ablish baseline architecture and review for weaknesses (e.g., use of Common Weakness VE)) and susceptibility to attack (e.g., use of Common Attack Pattern Enumeration and APEC)), and likelihood of attack success considering each detected weakness; identify p points and mission impacts. Consider which families of automated SwA engineering tools vulnerability or weakness detection.
- Review architecture and design for adherence to secure design principles and assess soundr decisions considering likely means of attack; programming language choices; development frameworks; and use of open source software, etc.
- Identify and mitigate technical risks through competitive prototyping while engineering in prototypes may be physical or math models and simulations that emulate expected perform concepts may require scaled models to reduce uncertainty too difficult to resolve purely by emulation. SW prototypes that reflect the results of key trade-off analyses should be demor TMRR phase. These demonstrations will provide SW performance data (e.g., latency, secu integration of legacy services, graceful function degradation and re-initiation, and scalabili decisions as to maturity; further, EMD estimates (schedule and life cycle cost) often depen components developed in TMRR; therefore to prevent technical debt, SwA considerations must have been taken into account.
- Develop a comprehensive system-level architecture, then design (address function integrity, assurance of the functional breakout, function interoperation, and separation of function) that covers the full scope of the system in order to maintain capabilities across multiple releases and provide the fundamental basis to fight through cyberattack. The program focused on a given SW build/release/increment may only produce artifacts for that

Systems Engineering Technical Review Success Criteria

Objective	SwA Success Criteria
Preliminary Design Review (PDR)	
Recommendation that allocated baseline fully satisfies user requirements and developer ready to begin detailed design with acceptable risk. Allocated baseline is established such that the design provides sufficient confidence that the program demonstrates a high likelihood of accomplishing its intended mission, including in a cyber-contested environment. Preliminary design and basic system architecture support capability need and affordability target achievement.	• Determine that baseline fully satisfies user requirements, with assurance engineered in. • Determine that likely means of attack through software have been assessed and used in architecture and design implementation. • Review architecture and design against secure design principles; including system element isolation, least common mechanism, least privilege, fault isolation, input checking and validation. Consult JFAC planning tools, best practices in architecture and design, and guidance. • Determine if initial SwA Reviews and Inspections from prior SETR activities capture planning and requirements appropriately, including assurance. • Confirm that SwA requirements that were previously mapped from tactical use threads, mission threads, system requirements, and system interoperability requirements, are mapped to module test cases and to the final acceptance test cases. • Establish automated regression testing procedures and tools as a core process, and assure regression testing is conducted for remediated vulnerabilities, defects, and weaknesses.

PM's Guidebook for SwA Activities



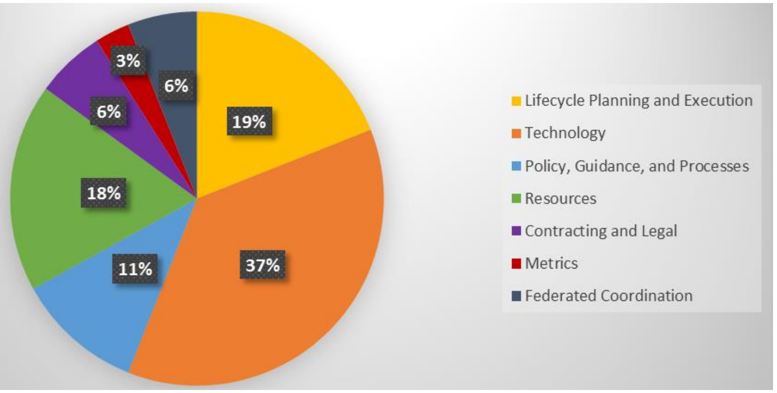
To be published by SEI.

Upcoming Journal of Cyber Security and Information Systems article:
"Engineering SwA into Weapon Systems during the DoD Acquisition Life Cycle"

What's Going on Now? (3 of 3)

In July 2016, the JFAC SwA Technical Working Group identified **63 DoD capability gaps** that prevent the effective planning and execution of software assurance within the DoD acquisition process. The gaps were organized into seven categories:

<u>Gap Examples:</u>
2.2.2 - SwA requirements lacking in system requirements
5.2.1 - Lack of SwA training for Program Managers
6.1 - Lack of definitive contract language for SwA planning and execution activities, as early in the lifecycle as possible

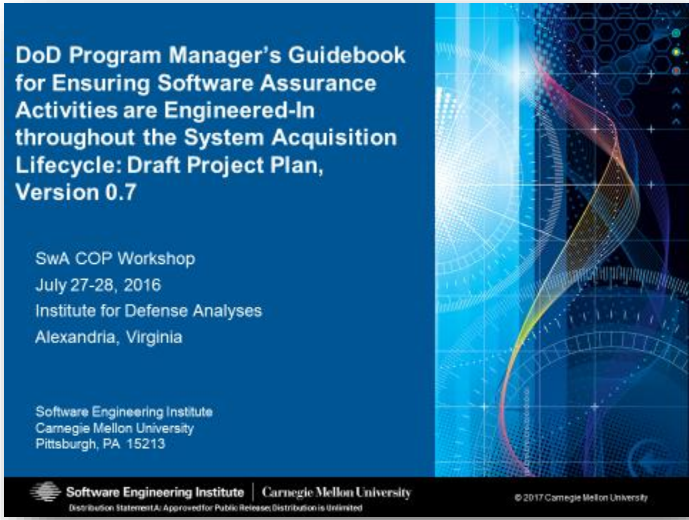


As chair of the JFAC Steering Committee, Ms. Kristen Baldwin, Acting Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), approved the analysis* and directed the Technical Working Group to **develop a strategy to address the identified gaps**. DASD(SE)'s JFAC lead, Mr. Tom Hurt, supported the **NDIA-sponsored joint industry-government workshop**.

*Distribution C, available upon request.

What's Next?

- **DoD Program Manager's Guidebook for Integrating Software Assurance Engineering Activities into the System Acquisition Life Cycle**
  - To be written and published by SEI in collaboration with JFAC SwA Technical WG
  - Partner Document: Software Developers Guidebook
- **DASD(SE) Activities**
  - FY18 Business Case Analysis for SwA Tools
- **JFAC website on SIPR, JWICS**
  - One-stop shop for SwA tools and best practices
  - New S&T and Assessment Knowledge Base portals
  - https://jfac.army.mil
- **Develop JFAC Full Operational Capability (FOC) strategy**
  - Improve DoD SwA throughout Lifecycle Planning, Execution and Sustainment
  - Linking Sustainment to Early Program Development



Conclusion

- **DoD has been focused on software assurance for over a dozen years.**
  - DASD(SE) leads the development and implementation of the supporting best practices, guidance, tools, and workforce competencies to ensure PMs have the means to mitigate SwA vulnerabilities and risk.
- **The JFAC's goal is to provide DoD programs a one-stop shop to request, evaluate, and obtain resources to improve their software assurance practice.**
  - SwA analysis tool license distribution and management
  - Service providers for programs' SwA work; SMEs focused on hard problems
  - SwA best practices
- **JFAC and DoD SwA COP is addressing key software assurance gaps.**
  - Developing FOC strategy to execute as resourcing becomes available

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace

http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering

http://www.acq.osd.mil/se

For Additional Information

Mr. Thomas Hurt

ODASD, Systems Engineering

571-372-6129

thomas.d.hurt.civ@mail.mil

Digital Engineering and Engineered Resilient Systems (ERS)

Mr. Robert Gold
Director, Engineering Enterprise
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 26, 2017

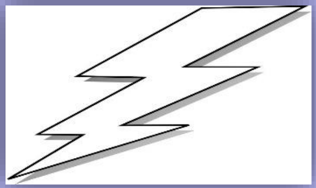
History

1st Industrial Revolution

MECHANICAL

Use of mechanical production powered by water and steam

2nd Industrial Revolution



ELECTRICAL

Use of mass production powered by electrical energy

3rd Industrial Revolution

INFORMATION TECHNOLOGY

Use of electronics and IT to further automation

4th Industrial Revolution

DIGITAL

Use of a digitally connected end-to-end enterprise

1800

1900

2000

TODAY

Traditional Models and Simulations (M&S)

Simulation Based Acquisition (SBA)

Model-Based Systems Engineering (MBSE)

DIGITAL ENGINEERING (DE)

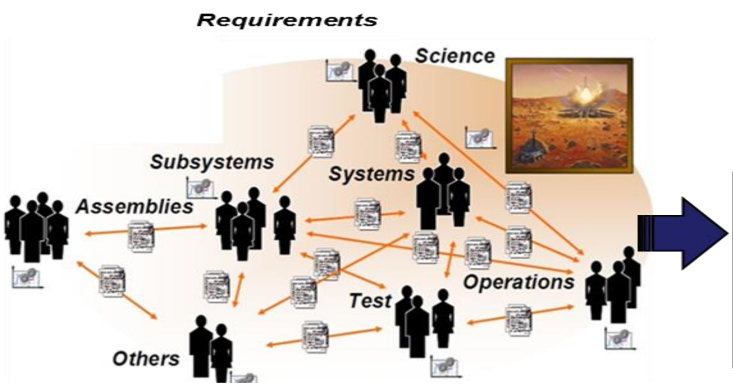
Digital Engineering: MBSE approach for DoD

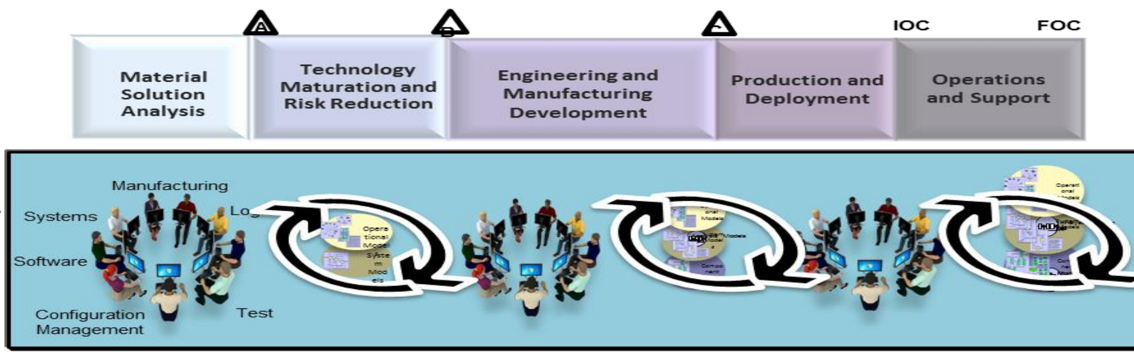
Current State

- Our workforce uses stove-piped data sources and models in isolation to support various activities throughout the life-cycle
- Current practice relies on standalone (discipline-specific) models
- Communication is through static disconnected documents and subject to interpretation

Future State

- Digital Engineering moves the engineering discipline towards an integrated model-based approach
  - Through the use of digital environments, processes, methods, tools, and digital artifacts
  - To support planning, requirements, design, analysis, verification, validation, operation, **and/or** sustainment of a system
- Digital Engineering ecosystem links our data sources and models across the lifecycle
  - Provides the authoritative source of truth





Current: Stove-piped models and data sources

Future: Digital Engineering Ecosystem

ERS Products in Digital Engineering Context

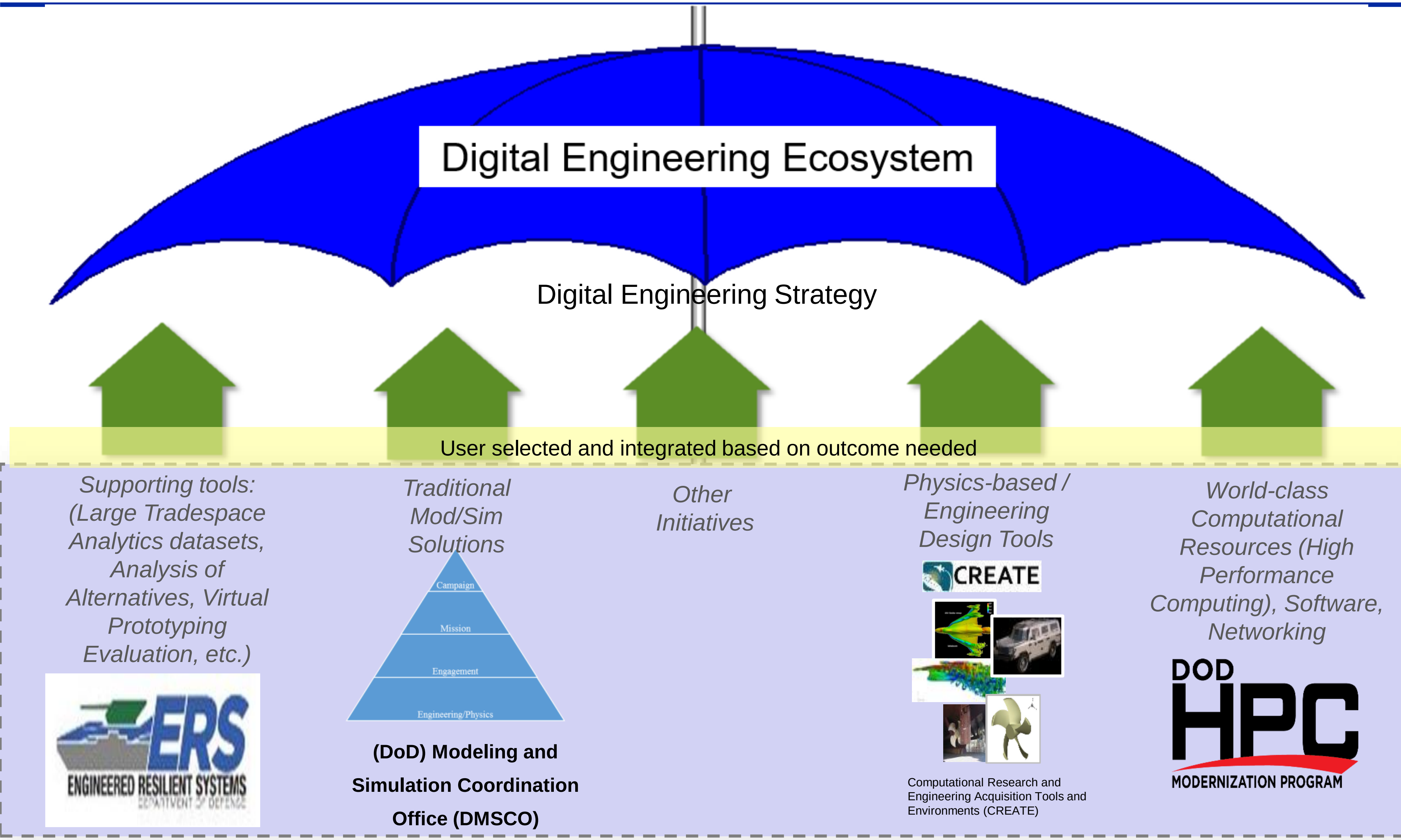
Digital Engineering

- **Digital Engineering vision moves the engineering discipline towards an integrated model-based approach through the use of digital environments, processes, methods, tools, and digital artifacts**
- **Model is a representation of reality**
  - Model is ‘composed of’ data, algorithms and/or processes
  - Computable or used in a computation

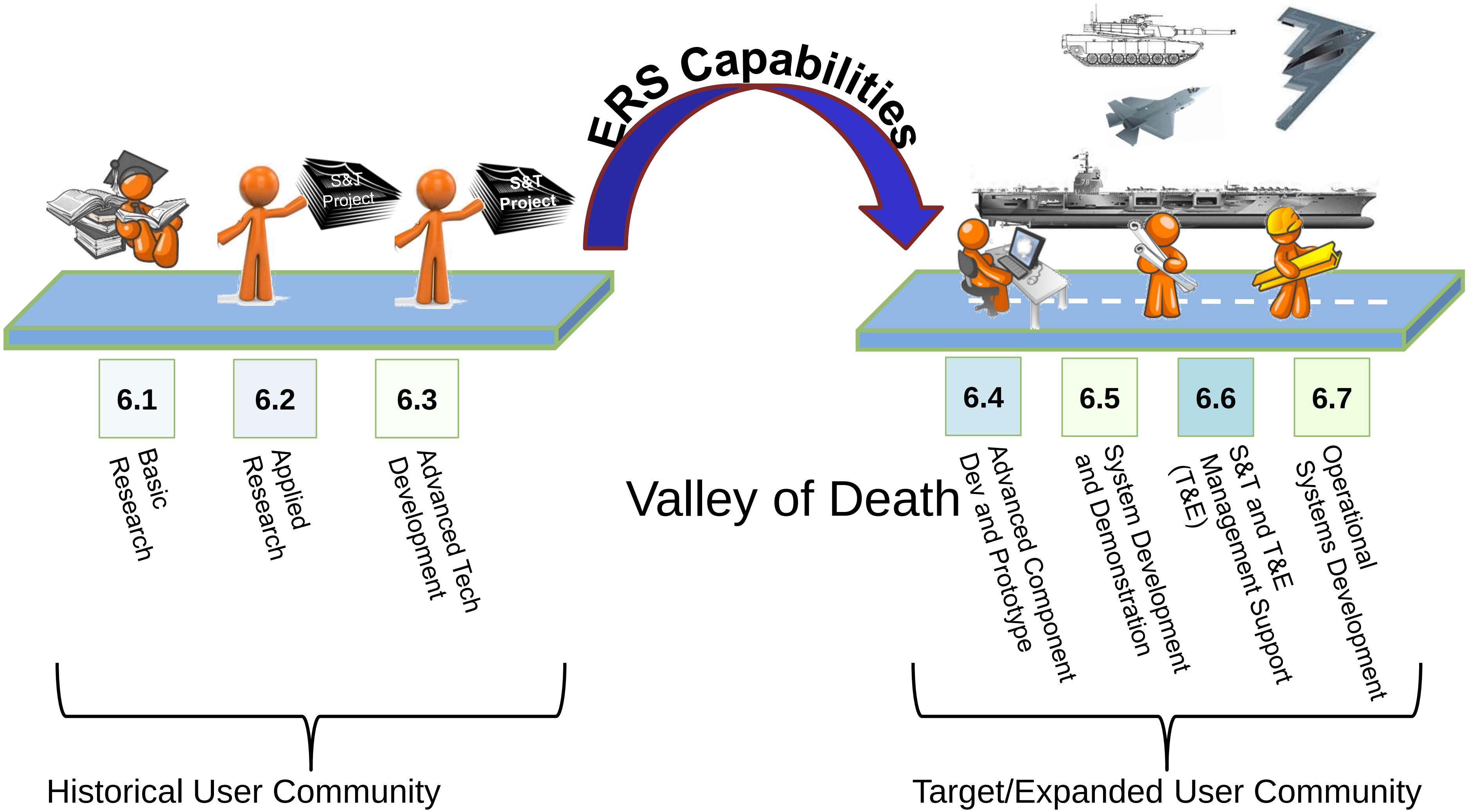
ERS

- **Engineered Resilient Systems (ERS) combines advanced engineering techniques with high-performance computing to develop concepts and tools that significantly amplify design options examined**
- **Develop/Integrate advanced engineering tools for efficient, integrated design and development across the full range of the product lifecycle**

Digital Engineering Relationships

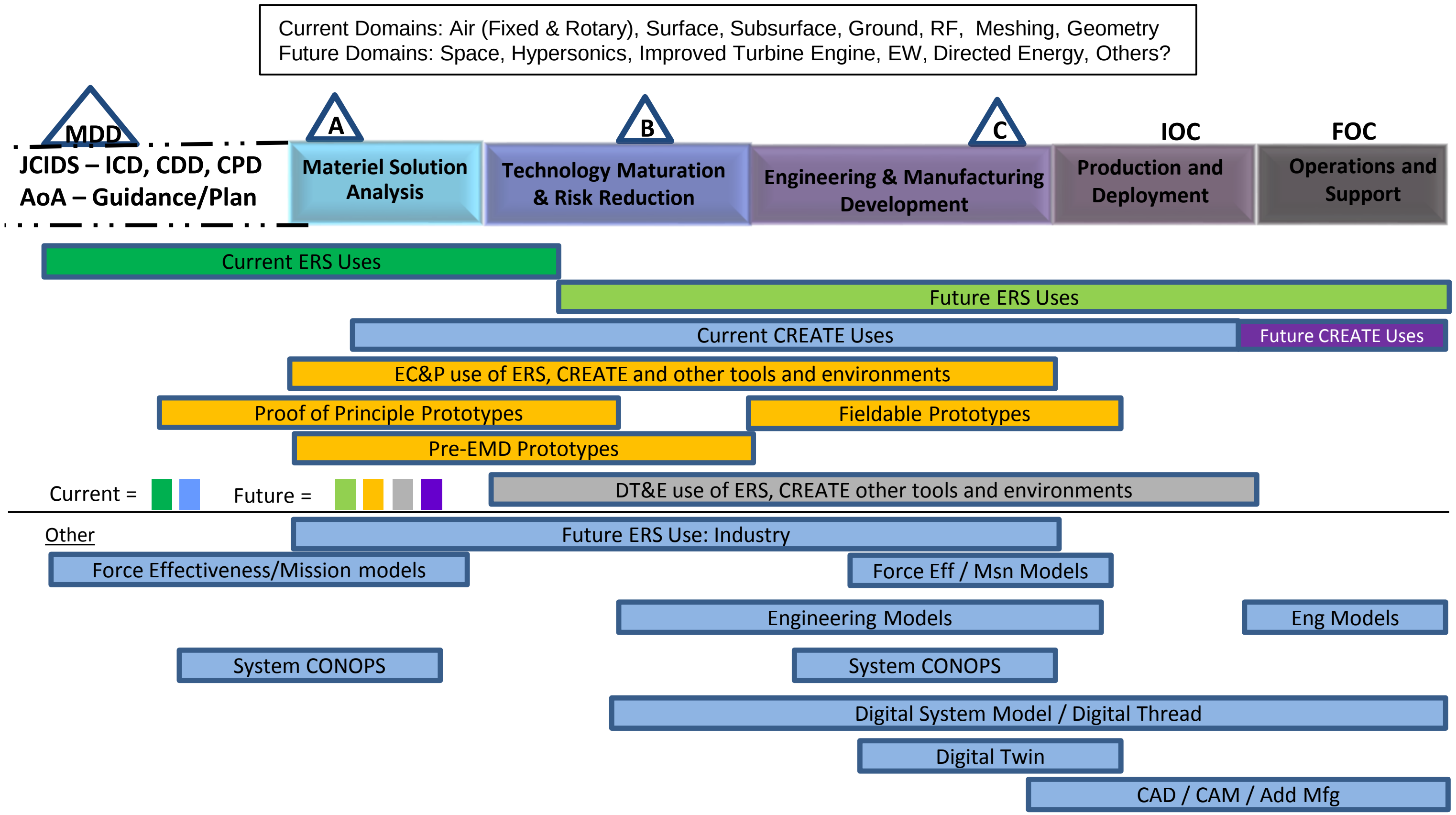


Transitioning S&T to Engineering & Acquisition



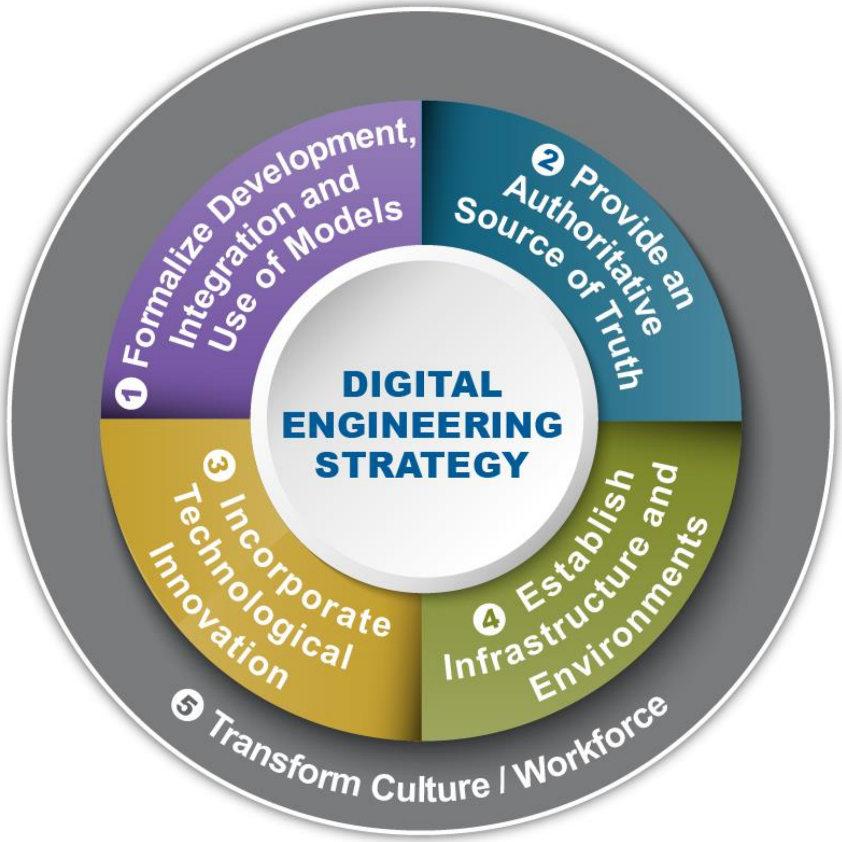
DRAFT Vision for ERS, CREATE, et al (crossing the Valley of Death)

DRAFT DRAFT



Digital Engineering Strategy: Five Goals

1. Formalize the **development, integration and use of models** to inform enterprise and program decision making
2. Provide an enduring **authoritative source of truth**
3. Incorporate **technological innovation** to improve the engineering practice
4. Establish supporting **infrastructure and environments** to perform activities, collaborate, and communicate across stakeholders
5. Transform a **culture and workforce** that adopts and supports Digital Engineering across the lifecycle



Drives the engineering practice towards improved agility, quality, and efficiency, resulting in improvements in acquisition

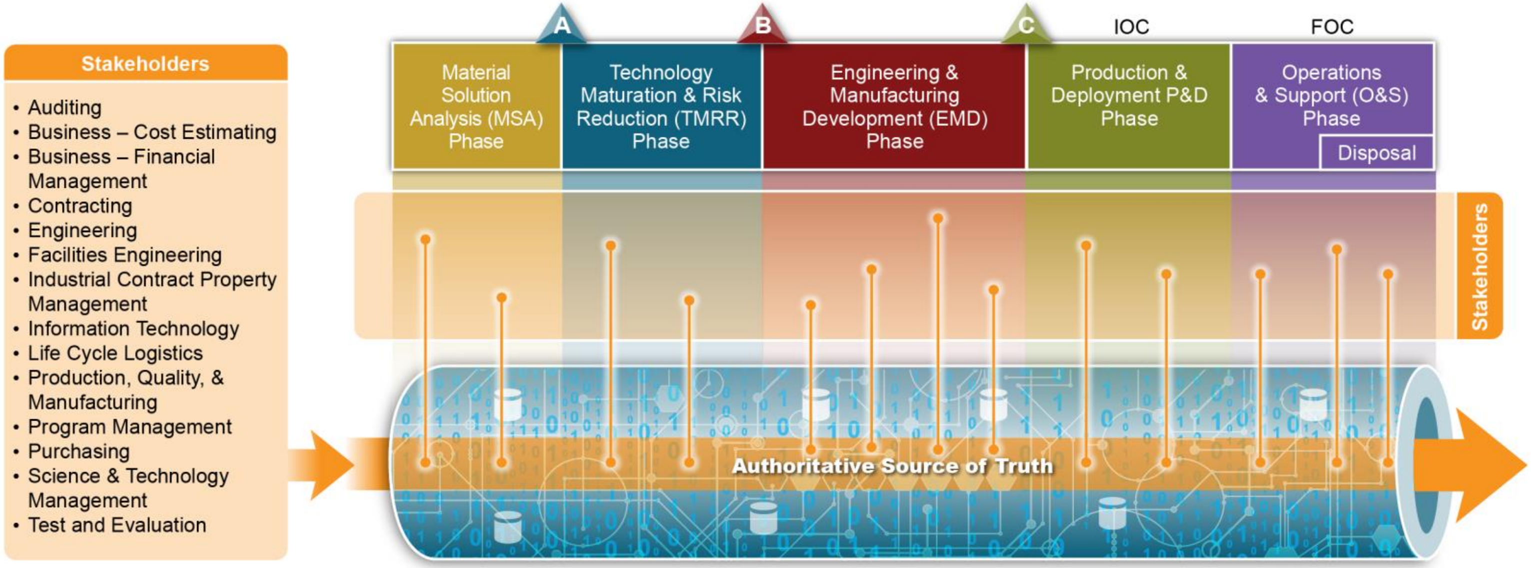
Goal #1: Formalize Development, Integration & Use of Models

ERS in DE Goal 1:

- Use of models to replace the sequential, fixed requirement approach to design
- Use of models will enable prototyping, experimenting and testing of solutions virtually before physical prototypes and full scale systems are available
- Use of evolving models will allow analysis of design options to be shifted left in the lifecycle
- Understand how to defeat a concept through inverse modeling

Models as the cohesive element across a system's lifecycle

Goal #2: Provide an Authoritative Source of Truth



ERS in DE Goal 2:

- Models are inherently more adaptable across mission sets and environments
- The authoritative sources of truth means ground truth
- ERS is fast and accurate enough to understand and mitigate risk in large, complex, and integrated data set

Right information, right people, right uses, right time

Goal #3: Incorporate Technological Innovation

- ❖ **Big Data and Analytics**
- ❖ **Cognitive Technologies**
- ❖ **Computing Technologies**
- ❖ **Digital-to-Physical Fusion Technologies**

ERS in DE Goal 3:

- Explore new concepts to integrated advanced engineering models
- Replace intensive manual processes to stitch data and artifacts together with workflow automation
- Explore new decision analytics that generate real alternatives that reflect the entire lifecycle demanded by increased digital engineering use
- Utilize machine learning to analyze massive and complex datasets containing a variety of data types from a multitude of sources
- Architecturally integrated with knowledge management

Harness technology, new approaches, and human-machine collaboration to enable an end-to-end digital enterprise

Goal #4: Establish Infrastructure & Environments

ERS in DE Goal 4:

- Architect an overall data ecosystem on HPCs
- Build generalized and reusable workflow engine
- Build enterprise-level web portal
- Organize software tools around the data
- Create visualization techniques that support decision makers

Foundational support for Digital Engineering environments

Goals #5: Transform Culture and Workforce

ERS in DE Goal 5:

- Understand that migrating to a digital ecosystem does not remove the responsibility from the users to select, manage, govern and use the tools appropriately
- Gain confidence in performing activities in a collaborative, integrated, digital model-based environment
- Learn to articulate the problem, workflow, and model boundary conditions to a third party
- Build understanding in how to appropriately reduce reliance on physical experimentation

Institutionalize Digital Engineering across the acquisition enterprise

There Is Much More to Do…

- **Publish the Digital Engineering Strategy**
  - Support development of implementation guidance/direction in Services/Agencies
  - Follow with policy?
- **Finish the Digital Engineering Starter Kit**
  - Continue development; share/obtain feedback on digital artifact use
- **Engage with Acquisition Programs**
  - Establish criteria for use of Digital Engineering artifacts for decision points
- **Update Competencies across Acquisition Curricula**
  - Identify Digital Engineering education and training outside of acquisition curricula
- **Update Policy and Guidance (Engineering, et al)**
  - Develop/update governance processes, policy, guidance and contracting language
- **Transform Acquisition Practice**
  - Engage acquisition users
  - Incorporate rigor from Digital Engineering practices and artifacts into system lifecycle activities

Instantiation of Digital Engineering practice is necessary to meet new threats, maintain overmatch, and leverage technology advancements

Systems Engineering: Critical to Defense Acquisition

Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Mr. Robert Gold

ODASD, Systems Engineering

703-695-3155

robert.a.gold4.civ@mail.mil

Digital Engineering Overview

Digital Engineering: An integrated digital approach that uses authoritative sources of systems' data and models as a continuum across disciplines to support lifecycle activities from concept through disposal.

- **Background**
  - Dynamic operational and threat environments
  - Growth in system complexity and risks
  - Linear acquisition process that lacks agility and resiliency
  - Cost overruns and delayed delivery of capabilities to the warfighter
  - Current practices can't keep pace with innovation and technology advancements
- **Need**
  - Outpace rapidly changing threats and technological advancements
  - Deliver advanced capabilities more quickly and affordably with improved sustainability to the warfighter
  - Foster a culture of innovation

Digital Engineering transforms the way the DoD innovates and operates

Digital Models Have Incredible Potential

DoD needs:

- **Flexible designs that adapt and are resilient to unknown missions and threats**
- **Cost and affordability as quantifiable attributes of the trade space**
- **Systems of Systems, and Enterprise, contexts in order to respond to multiple stakeholders**
- **A balance between agility in acquisition and rigorous analysis and data**
- **Critical information appropriately protected while designing for interoperability**
- **Support in significantly diverse domains**

Balancing these axioms is challenging.
It drives the need for, and use of digital models to:

- **Maintain consistency about the system**
- **Integrate technical and non-technical drivers**
- **Understand the various perspectives on the system under development**

Models are advancing the STATE OF PRACTICE of SE

Digital Engineering (DE) and Computational Research and Engineering Acquisition Tools and Environments (CREATE)

Ms. Phil Zimmerman
Deputy Director, Engineering Tools and Environments
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

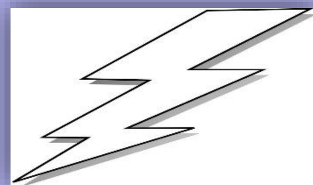
History

1st Industrial Revolution

MECHANICAL

Use of mechanical production powered by water and steam

2nd Industrial Revolution



ELECTRICAL

Use of mass production powered by electrical energy

3rd Industrial Revolution

INFORMATION TECHNOLOGY

Use of electronics and IT to further automation

4th Industrial Revolution

DIGITAL

Use of a digitally connected end-to-end enterprise

1800

1900

2000

TODAY

Traditional Models and Simulations (M&S)

Simulation Based Acquisition (SBA)

Model-Based Systems Engineering (MBSE)

DIGITAL ENGINEERING (DE)

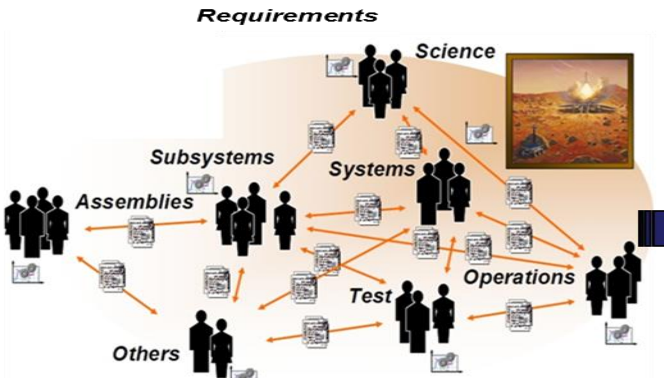
Digital Engineering: MBSE approach for DoD

Current State

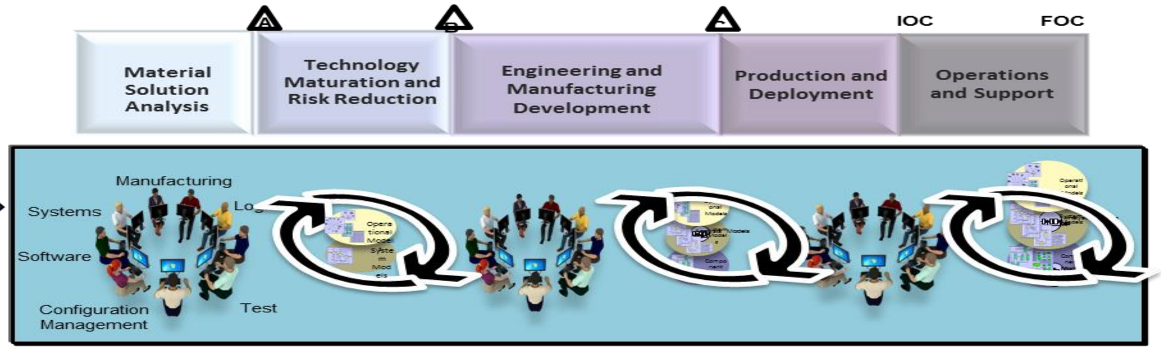
- Our workforce uses stove-piped data sources and models in isolation to support various activities throughout the life-cycle
- Current practice relies on standalone (discipline-specific) models
- Communication is through static disconnected documents and subject to interpretation

Future State

- Digital Engineering moves the engineering discipline towards an integrated model-based approach
  - Through the use of digital environments, processes, methods, tools, and digital artifacts
  - To support planning, requirements, design, analysis, verification, validation, operation, **and/or** sustainment of a system
- Digital Engineering ecosystem links our data sources and models across the lifecycle
  - Provides the authoritative source of truth



Current: Stove-piped models and data sources



Future: Digital Engineering Ecosystem

CREATE Products in Digital Engineering Context

Digital Engineering

- **Digital Engineering vision moves the engineering discipline towards an integrated model-based approach through the use of digital environments, processes, methods, tools, and digital artifacts**
- **Model is a representation of reality**
  - Model is ‘composed of’ data, algorithms and/or processes
  - Computable or used in a computation

CREATE

- **CREATE program develops and deploys validated physics-based High Performance Computing (HPC) applications to enable DoD engineers to implement and execute the digital engineering paradigm for major DoD platforms (naval, air, & ground vehicles and RF antennas)**
- **Includes ability to construct and improve digital product models for weapon platforms**
  - Tools address all stages of the acquisition process

Digital Engineering Relationships

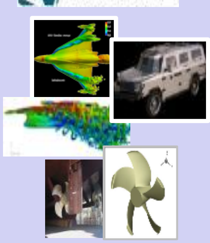
Digital Engineering Ecosystem

Digital Engineering Strategy

User selected and integrated based on outcome needed

Physics-based / Engineering Design Tools

CREATE



Computational Research and Engineering Acquisition Tools and Environments (CREATE)

World-class Computational Resources (High Performance Computing), Software, Networking

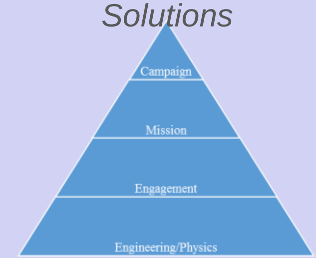
DOD HPC MODERNIZATION PROGRAM

Other Initiatives

Supporting tools: (Large Tradespace Analytics datasets, Analysis of Alternatives, Virtual Prototyping Evaluation, etc.)

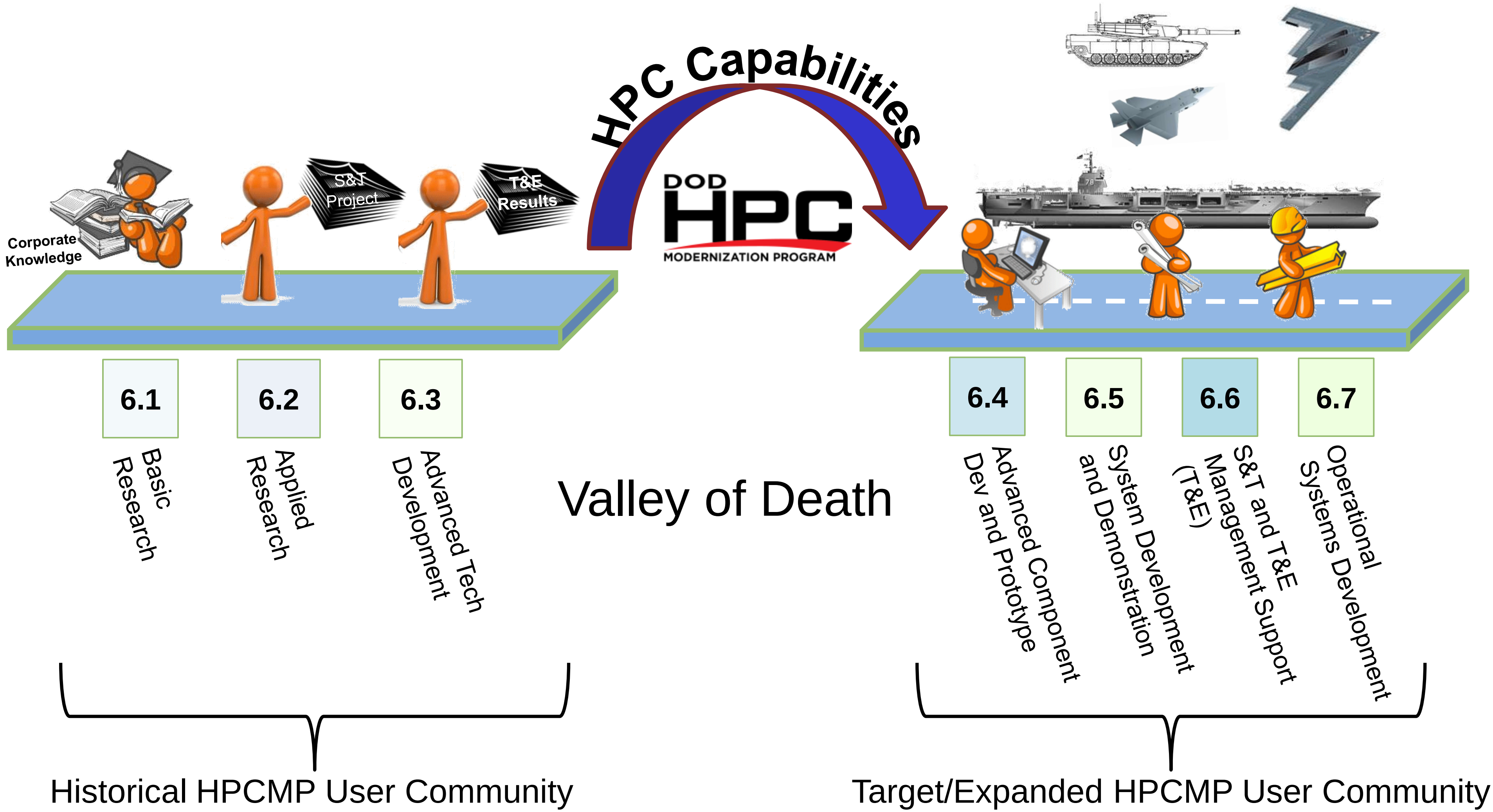
ERS ENGINEERED RESILIENT SYSTEMS DEPARTMENT OF DEFENSE

Traditional Mod/Sim Solutions



(DoD) Modeling and Simulation Coordination Office (DMSCO)

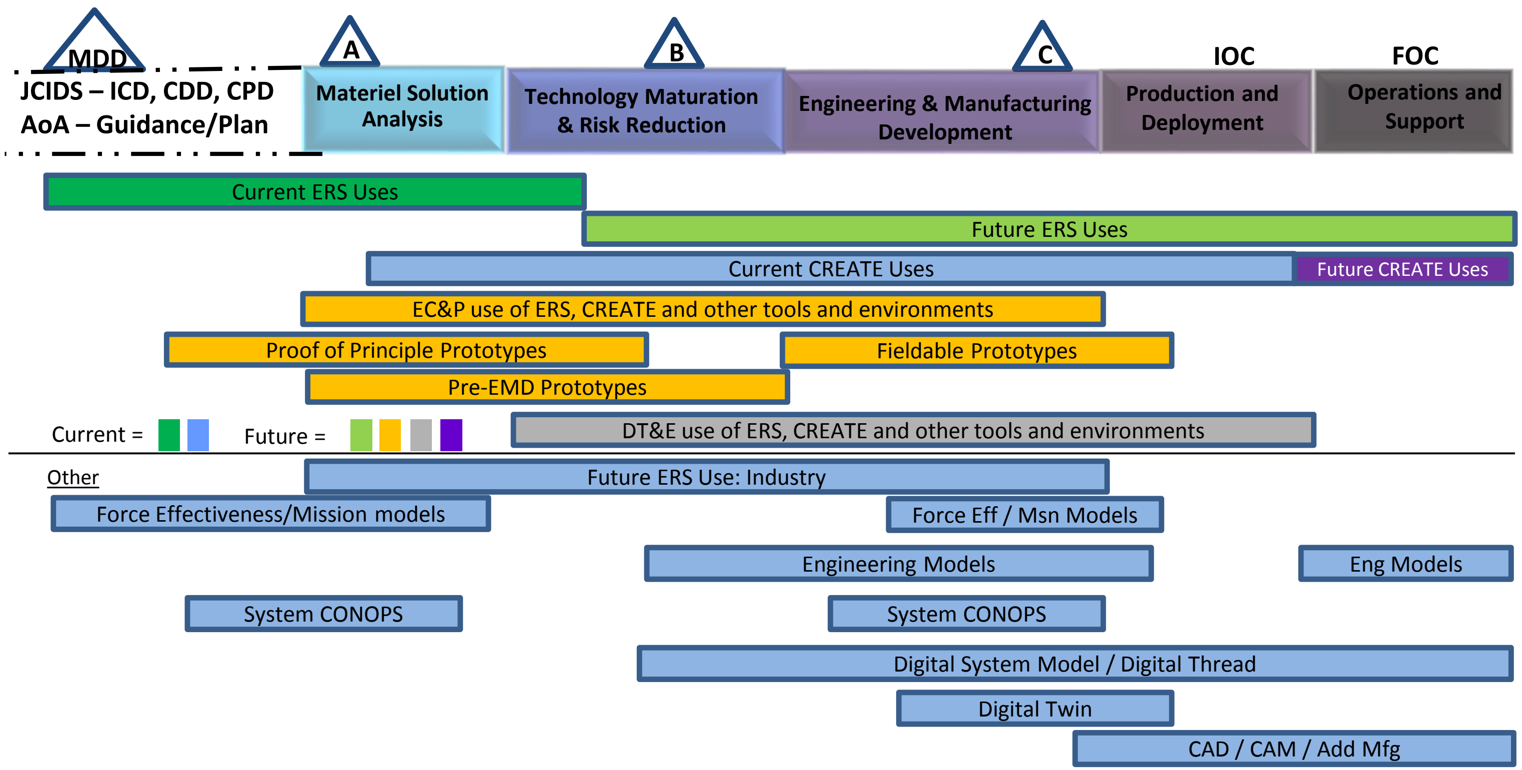
Transitioning S&T, T&E and Corporate Knowledge to Engineering & Acquisition



DRAFT Vision for ERS, CREATE, et al (crossing the Valley of Death)

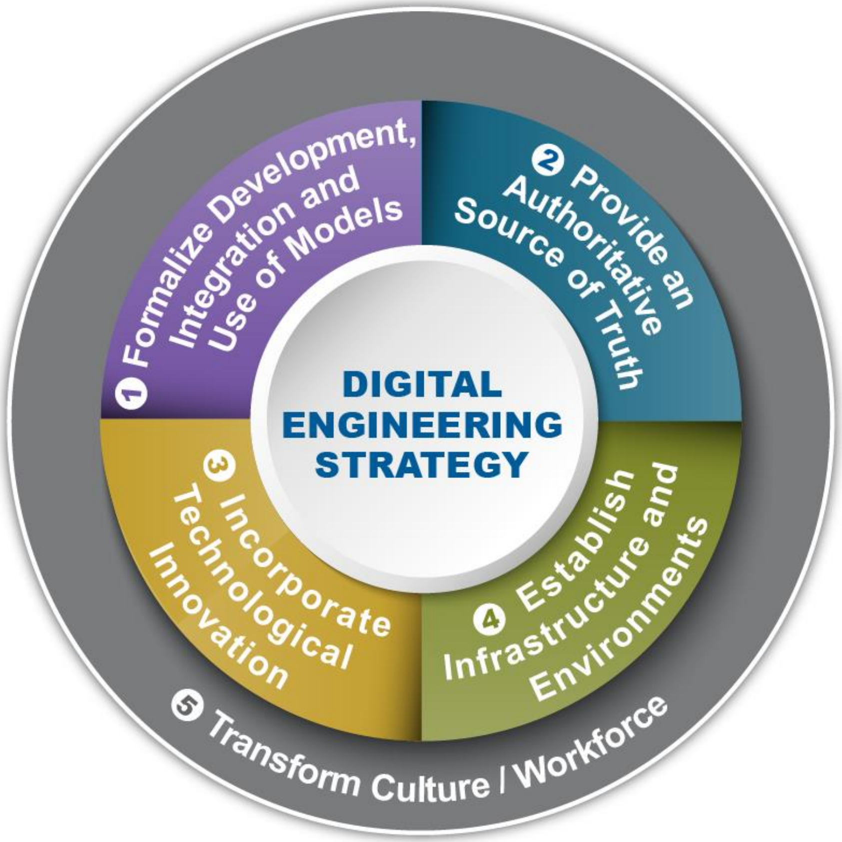
DRAFT DRAFT

Current Domains: Air (Fixed & Rotary), Surface, Subsurface, Ground, RF, Meshing, Geometry
Future Domains: Space, Hypersonics, Improved Turbine Engine, EW, Directed Energy, Others?



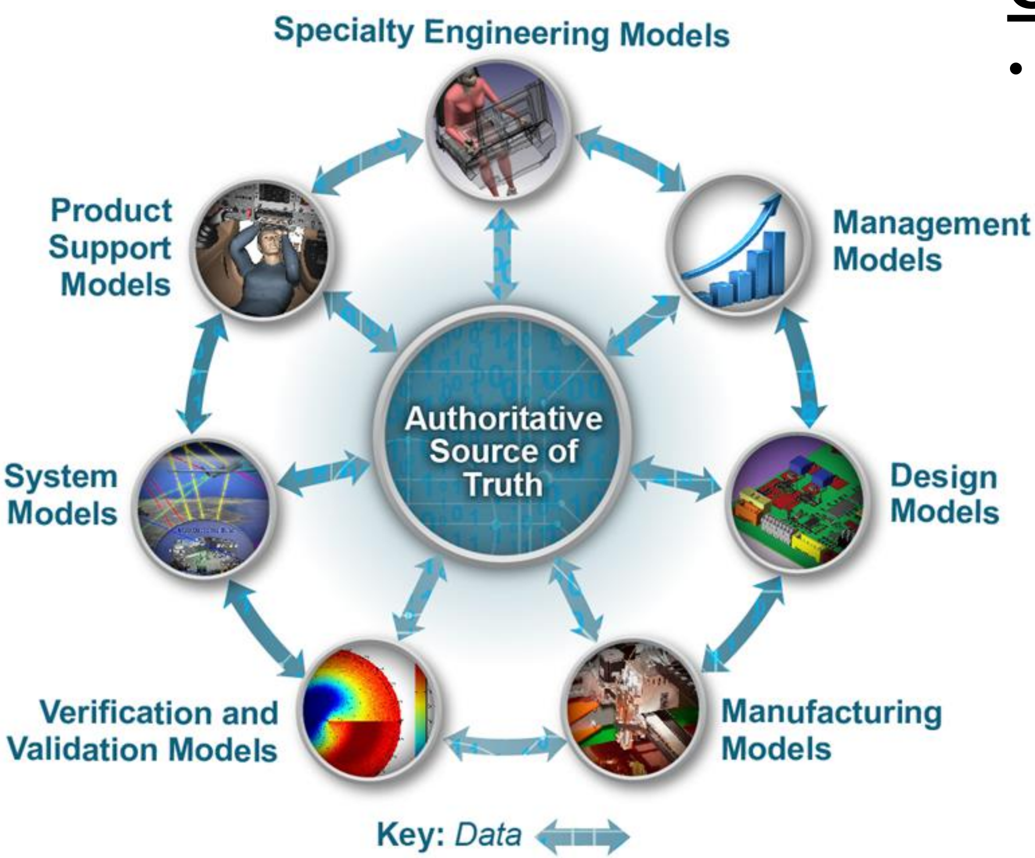
Digital Engineering Strategy: Five Goals

1. Formalize the **development, integration and use of models** to inform enterprise and program decision making
2. Provide an enduring **authoritative source of truth**
3. Incorporate **technological innovation** to improve the engineering practice
4. Establish supporting **infrastructure and environments** to perform activities, collaborate, and communicate across stakeholders
5. Transform a **culture and workforce** that adopts and supports Digital Engineering across the lifecycle



Drives the engineering practice towards improved agility, quality, and efficiency, resulting in improvements in acquisition

Goal #1: Formalize Development, Integration & Use of Models

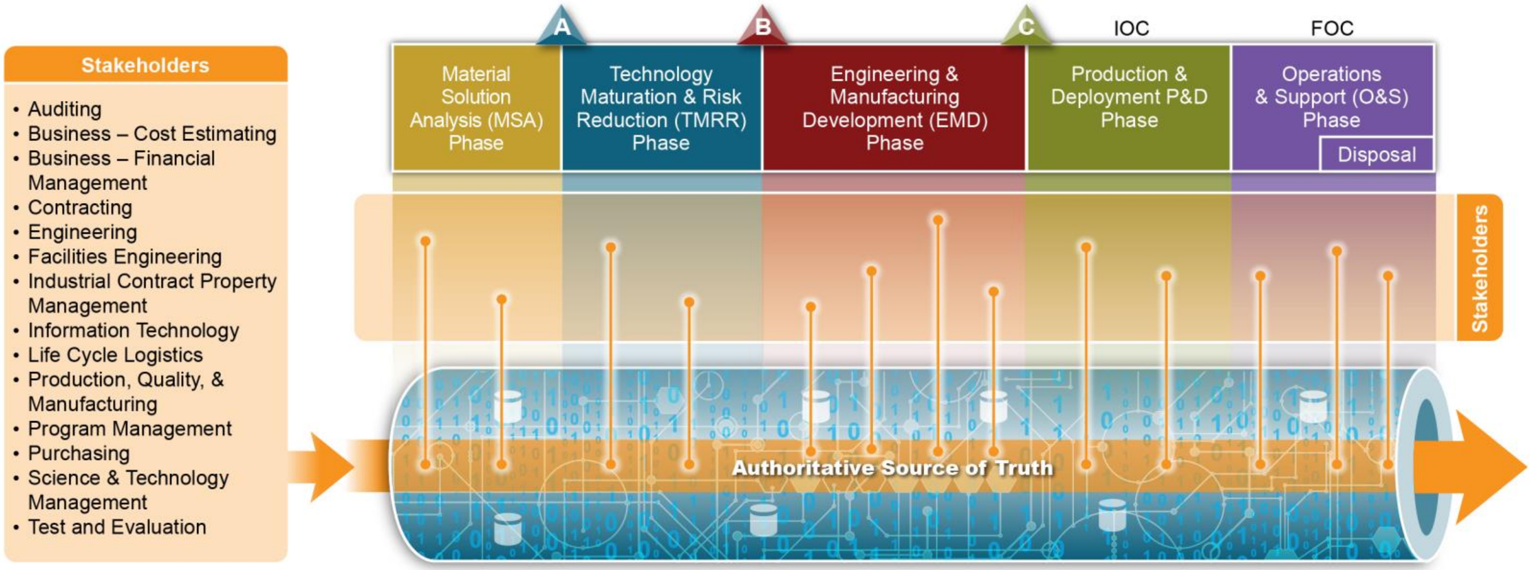


CREATE in DE Goal 1:

- Develop, deploy and support physics-based software applications that enable DoD engineers to rapidly:
  - Develop digital product models (virtual prototypes) for weapon systems which can be used to populate design spaces
  - Analyze the performance of the of the systems, using medium- and high-fidelity physics-based HPC tools, identifying and fixing system design defects and performance shortfalls thus reducing rework, and costs, risks, and schedule, and improving performance for all stages of the acquisition process

Models as the cohesive element across a system's lifecycle

Goal #2: Provide an Authoritative Source of Truth



CREATE in DE Goal 2:

- Develop and deploy verified and validated physics-based HPC tools that include: all important effects, accurate solution algorithms, and model the complete system i.e. everything needed to accurately predict the performance in short enough compute times for parameter studies

Right information, right people, right uses, right time

Goal #3: Incorporate Technological Innovation

❖ **Big Data and Analytics**

❖ **Cognitive Technologies**

❖ **Computing Technologies**

❖ **Digital-to-Physical Fusion Technologies**

CREATE in DE Goal 3:

- HPCMP eco-system employs innovative technologies (High Performance Computers, high speed networks and advanced software).
- DoD engineers develop innovative systems by rapidly and efficiently generating many design options; identifying the failures and successes; and improvements
- Use of small teams to take risks, fail early and quickly in order to identify successful product designs

Harness technology, new approaches, and human-machine collaboration to enable an end-to-end digital enterprise

Goal #4: Establish Infrastructure & Environments

CREATE in DE Goal 4:

- High Performance Computing Ecosystem:
  - Subject matter experts from relevant stakeholders
  - Validated and verified data for use in engineering and acquisition activities
  - HPC Distributed Resource Centers
  - High-bandwidth network (DREN)
  - Software applications (CREATE codes now and in the future)

Foundational support for Digital Engineering environments

Goals #5: Transform Culture and Workforce

CREATE in DE Goal 5:

- HPCMP Partnerships with Service Engineering Organizations
- Development and use of CREATE builds computationally skilled DoD workforce
- Training and support is provided for those accessing CREATE – over 180 DoD organizations with ~1400 users.
- CREATE software is being incorporated into Service Academy and other university curricula
- Regular release of upgraded software capability

Institutionalize Digital Engineering across the acquisition enterprise

There Is Much More to Do…

- **Publish the Digital Engineering Strategy**
  - Support development of implementation guidance/direction in Services/Agencies
  - Follow with policy?
- **Finish the Digital Engineering Starter Kit**
  - Continue development; share/obtain feedback on digital artifact use
- **Engage with Acquisition Programs**
  - Establish criteria for use of Digital Engineering artifacts for decision points
- **Update Competencies across Acquisition Curricula**
  - Identify Digital Engineering education and training outside of acquisition curricula
- **Update Policy and Guidance (Engineering, et al)**
  - Develop/update governance processes, policy, guidance and contracting language
- **Transform Acquisition Practice**
  - Engage acquisition users
  - Incorporate rigor from Digital Engineering practices and artifacts into system lifecycle activities

Instantiation of Digital Engineering practice is necessary to meet new threats, maintain overmatch, and leverage technology advancements

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Ms. Philomena Zimmerman

ODASD, Systems Engineering

571-372-6695

philomena.m.zimmerman.civ@mail.mil

NDIA System Engineering Conference
24 October 2017

Benjie Spencer
Chief Engineer, NOAA/National Weather Service

NOAA

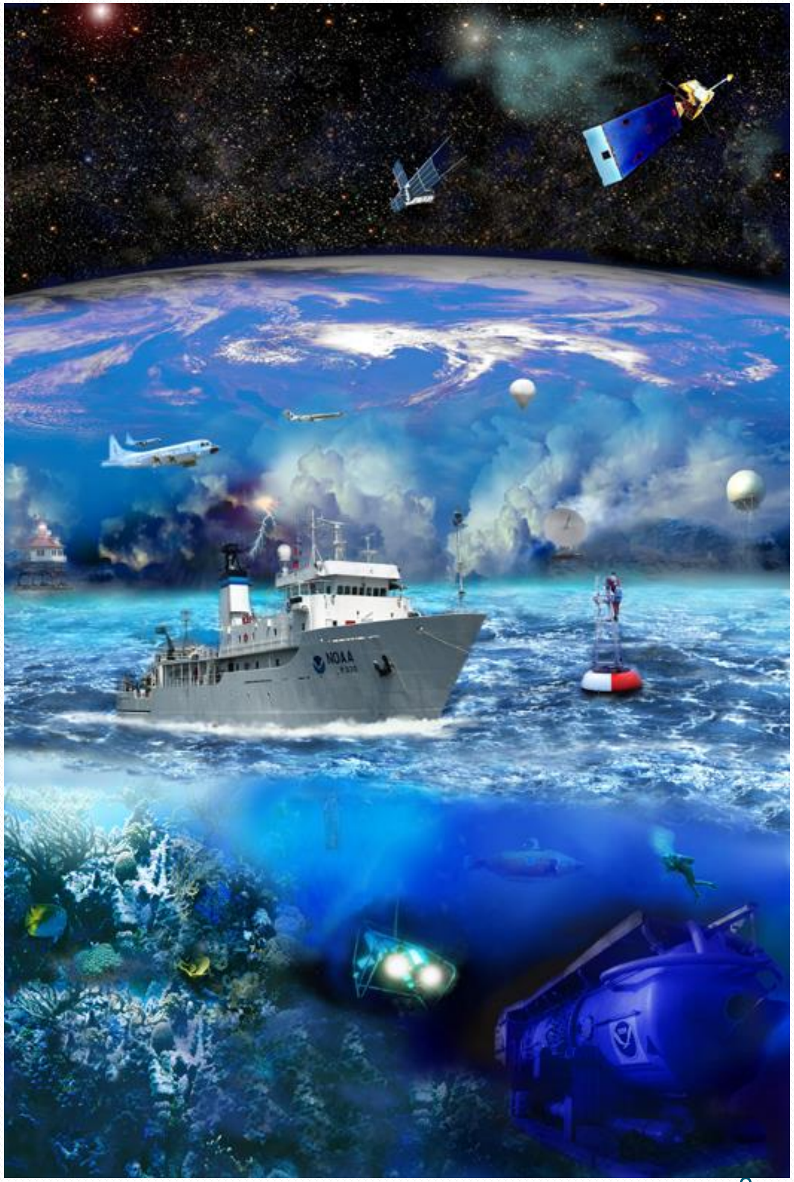
NOAA is an agency that enriches life through science. Our reach from sun to seafloor helps to keep citizens informed of the changing environment around them.

Mission: Science, Service, & Stewardship.

To *understand and predict changes in climate, weather, oceans, and coasts,*

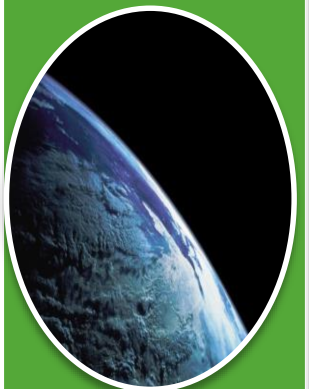
To *share that knowledge and information with others, and*

To *conserve and manage coastal and marine ecosystems and resources.*

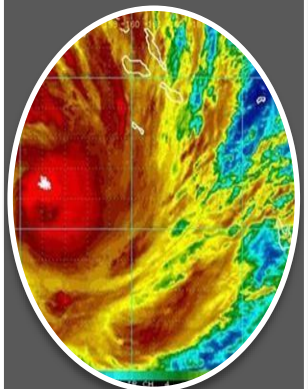


NOAA Line Offices

National Weather Service (NWS)

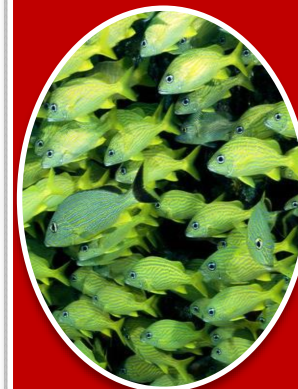


Oceanic and Atmospheric Research (OAR)



National Environmental Satellite Data & Information Service (NESDIS)

National Ocean Service (NOS)



National Marine Fisheries Service (NMFS)

Office of Marine and Aviation Operations (OMAO)

SCIENCE

SERVICE

STEWARDSHIP

NOAA's unique assets support our integrated mission

NOAA professionals

- 20,000 staff
  - 12,500 FTE
    - ~ 230 Engineers
  - NOAA Corps – the Nation's 7th Uniformed Service
  - 7,500 contractors
  - 18 National Labs & Science Centers

High Performance Computing

- 5 supercomputers

Observing Systems

- ~125 weather radars
- 10 satellites
- 3 buoy networks
- 210 tide gages

Ships and Aircraft

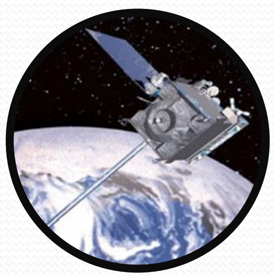
- 16 ships
- 9 aircrafts

Okeanos Explorer

NOAA G4 and P3

NOAA Employee Operating AWIPS

TAO Buoy



GOES

NOAA Observing Systems
(128)

Achievements

NEXRAD Backup Comms

- For a 10 year period from 2005 to 2015, the overall comms availability was 97% due to serve weather
- Implementation of 4G and VSAT Back Up Restores availability to 99.99% Reducing Downtime
  - Commercial T1 and Frame Relay service with auto fail-over (DoD and FAA radar data)
- Phased implementation approach
  - Networx contract extended in March 2017
  - Comms contract rebid in 2020 (unknown impact)
  - NEXRAD Software update in Build 18 to improve link stability & status reporting
- 84 sites installed
  - 11 NWS VSAT
  - 46 NWS 4G
  - 21 DoD 4G
  - 4 FAA 4G
  - 1 FAA VSAT

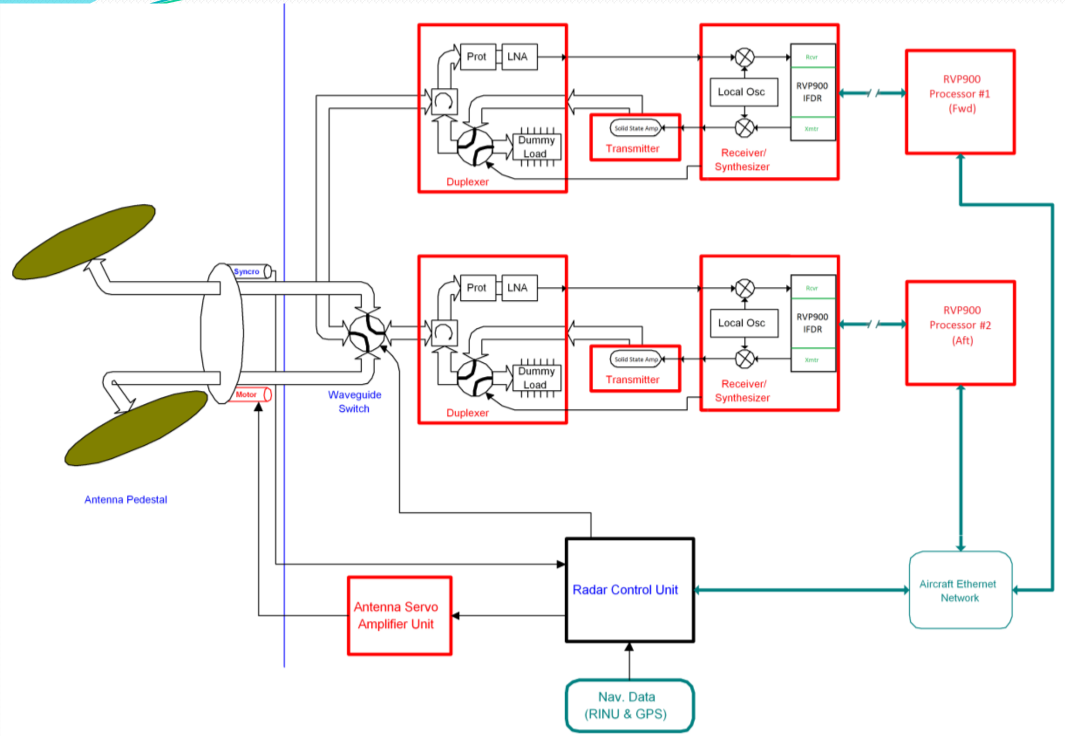
Joint NWS/DoD Radar Deployment to Puerto Rico

- **Hurricane Maria** severely damaged the FAA's WSR-88D Doppler Radar in PR. NWS, through the FEMA NRCC, requested DoD support to deploy two USMC tactical Doppler radars to re-establish coverage. The USMC radars were selected because of their ability to export NEXGEN Level 3 data.

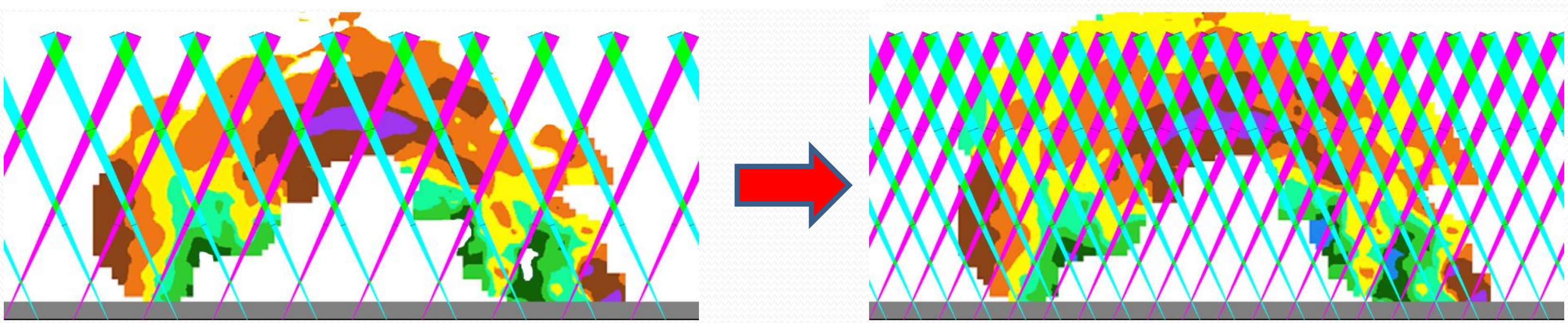
- With the support of the Navy PEO C4I PMW 120, Navy SPAWARS, Pacific, NORTHCOM, MARFORNORTH, and USMC 2MEF, an unprecedented joint engineering effort began to bring the X-band radar data into the NWS Advanced Weather Interactive Processing System (AWIPS, the primary forecasting support system for the NWS). The radars will be connected to NWS VSAT units to move the data into the NWS system where it can be utilized by forecasters in San Juan or at back-up forecast offices to provide life-saving forecasts and warnings.

- On 21 Oct 17, Marine forecasters and technicians will arrive with the radars in PR. They will link up with SPAWARS and NWS Radar Operations Center technicians to establish the two sites and begin the final efforts to assimilate the radar data into the NWS AWIPS. NWS will also support interim communications from the FAA's Terminal Doppler Weather Radar to the NWS AWIPS system to enable forecasters to utilize it for forecasts and warnings.

WP-3D Tail Doppler Radar Upgrade



- Completely dual system (Xmtrs, Rcvrs, Processors) for higher along-track resolution and redundancy
- 8 KW Solid State Power Amplifiers for improved sensitivity
  (5 dBZ -> -9 dBZ)
- Upgraded processors are the same as used in NOAA's NEXRAD WSR-88D ground radar
- Replacement antenna motors to double rotation speed and along-track resolution



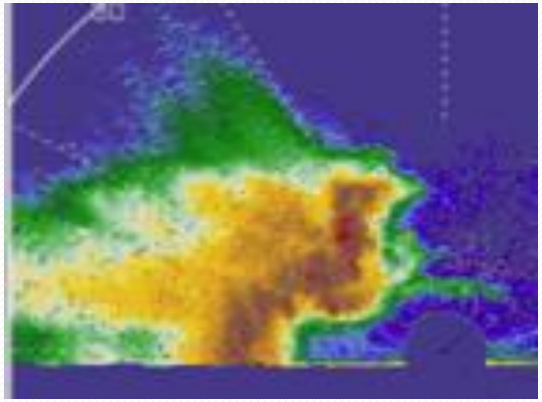
9

Tail Doppler Radar

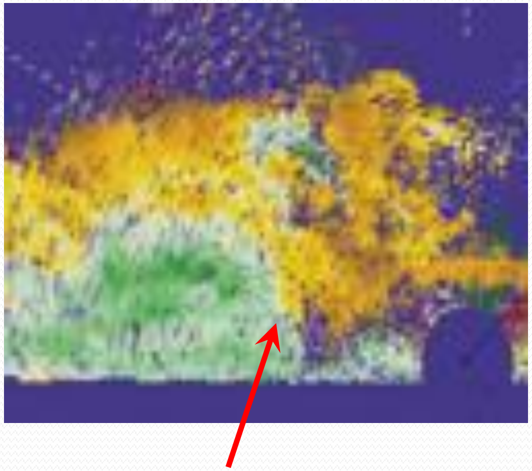
N42RF TDR Captures F0 Tornado Data on Vortex-SE Mission Flight

F0 Tornado from Ground Spotter

Reflectivity, showing very heavy rain and a strong inflow/updraft from the right



Doppler Velocity – Brown/orange away from aircraft and green/blue toward plane. Tornadic signature Is where the velocity direction changes

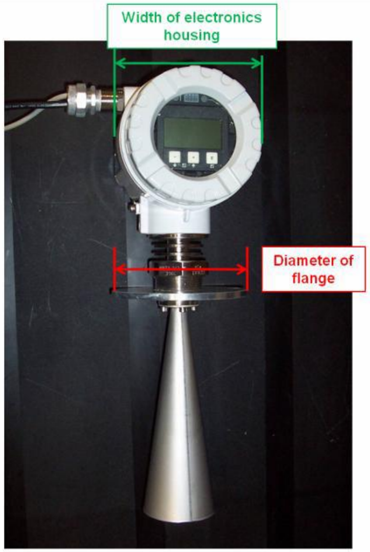


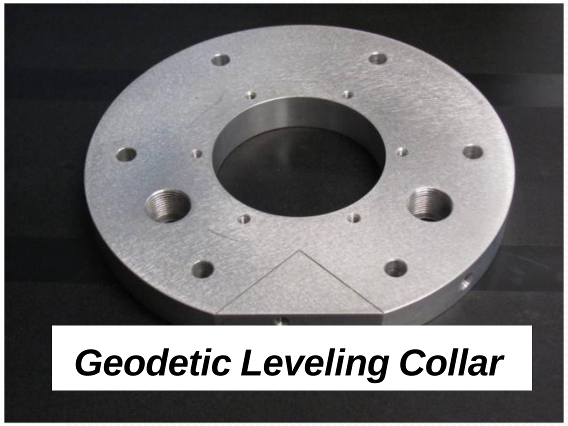
New TDR system is collecting research and operational data with higher sensitivity and resolution

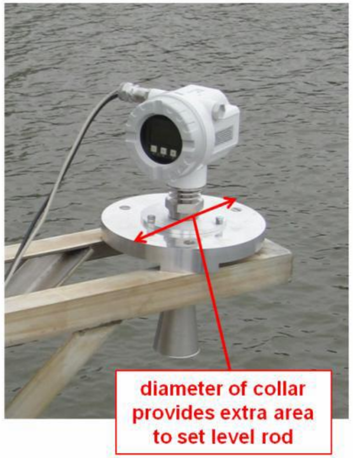
Transition to Operations

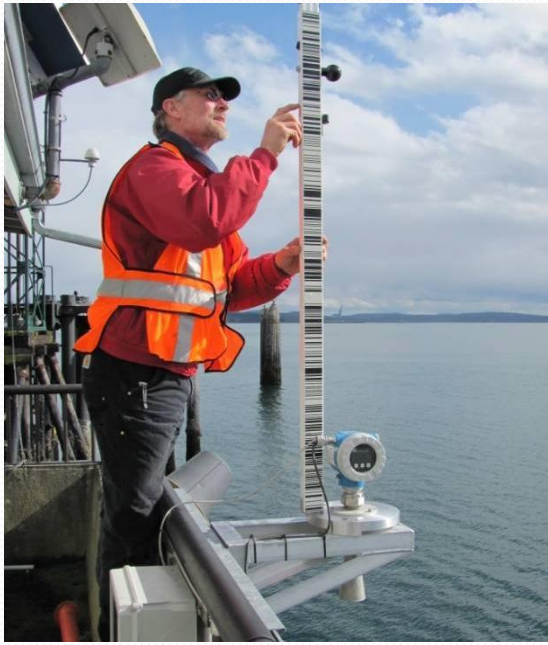
Micro-wave Water Level (MWWL) Measurement System

Mount Designs



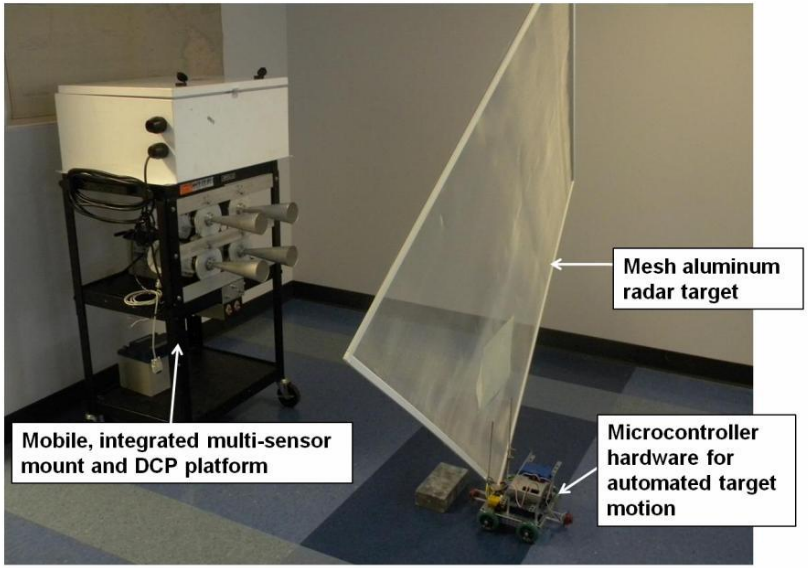






Laboratory Test Procedure and Facility

1) Fixed Target - Resolution Verification
2) Time Response Verification
3) Sensor Offset Derivation
4) Dynamic Liquid Tare test
5) Range Accuracy Verification



Saildrone 2017: Interdisciplinary Ocean Observations from the Arctic to the Tropics

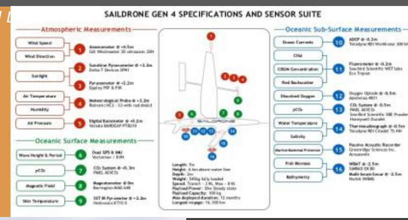
Christian Meinig[1], Edward Cokelet[1], Meghan Cronin[1], Jessica Cross[1], Alex De Robertis[3], Richard Jenkins[4], Carey Kuhn[3], Noah Lawrence-Slavas[1], Calvin Mordy[2], Phyllis Stabeno[1], Adrienne Sutton[2], Dongxiao Zhang[2], Jessica Crance[3], Jennifer Keene[2], Stacy Maener[1], Heather Tabisola[2]

[1]NOAA/Pacific Marine Environmental L... ans/PMEL, [3]NOAA/Alaska Fisheries Science Center, [4]Saildr...

TPOS 2020 Tropical Pacific Observing System

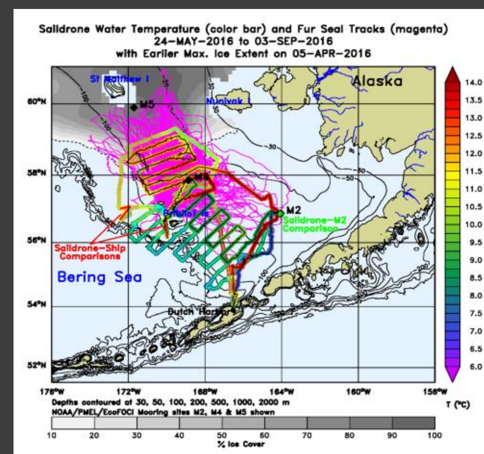
2017 Bering Sea & Chukchi Missions

- 3 Autonomous Surface Vehicles (ASVs)
- 2 integrated with Autonomous Surface Vehicle pCO_2 ($ASVCO_2$) sensor for Northern Chukchi Integrated Study
- 1 integrated with EK-80 echosounder for walleye pollock and northern fur seal study and passive acoustics
- ~3 month mission
- Deploy and recover from dock in Dutch Harbor, AK

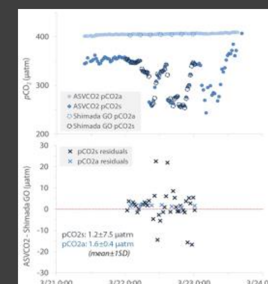


2017 Tropical Pacific Mission

- 2 Autonomous Surface Vehicles (ASVs) integrated with: Autonomous Surface Vehicle pCO_2 ($ASVCO_2$), ADCP, Heat Flux Sensor
- Participation in NASA SPURS II Field Campaign
- Climate quality comparison with instrumentation on ships, buoys and other platforms
- ~6 month mission
- Deploy and recover from dock in Alameda, CA

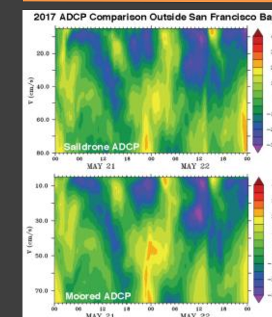


Carbon: TRL 7



- PMEL developed $ASVCO_2$ system measures pco2, pH
- 1-hour values transmitted via Iridium in near real time
- Compares favorably with ship and mooring observation testing completed off California

Ocean Current Profiling: TRL 5



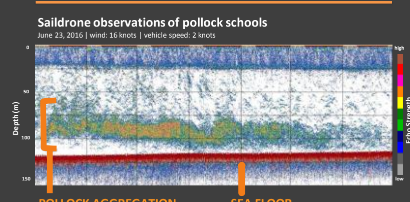
- Teledyne RDI Workhorse 300 kHz
- Dual GPS & Vectornav IMU
- Compares favorably with mooring observation testing completed off California

2016 Mission Results

Oceanography: TRL 5-9

- Measured 14 atmospheric and oceanic parameters
- 1-Hz sampling with 1-minute data Transmitted via Iridium in near real time
- Compares favorably with ship and mooring observations

Fisheries Acoustics: TRL 7



- Continuously measured fish acoustic backscatter with Kongsberg/Simrad AS echosounder
- High-quality measurements at wind speeds less than 20 knots
- Comparisons with research vessel indicate that shallow pollock react to ship noise

Fur Seal Tracking: TRL 7

- Tracked 30 satellite-tagged, adult-female fur seals as they foraged over ~70 days
- Saildrones spent 65 days covering fur-seal grid ~2 times
- Followed and recorded behavior and prey field of 2 fur seals for 1.3 and 2 days

Marine Mammal Acoustics: TRL 6

- Acousondes recorded 201 of 206 mission days and obtained ~5150 hours of recordings
- Saildrones spent 69 days within right whale critical habitat area and 12.5 days at two mooring locations for baseline acoustic comparisons
- Successful acoustic detection of killer whale with possible detection of right, fin and humpback whale(s)

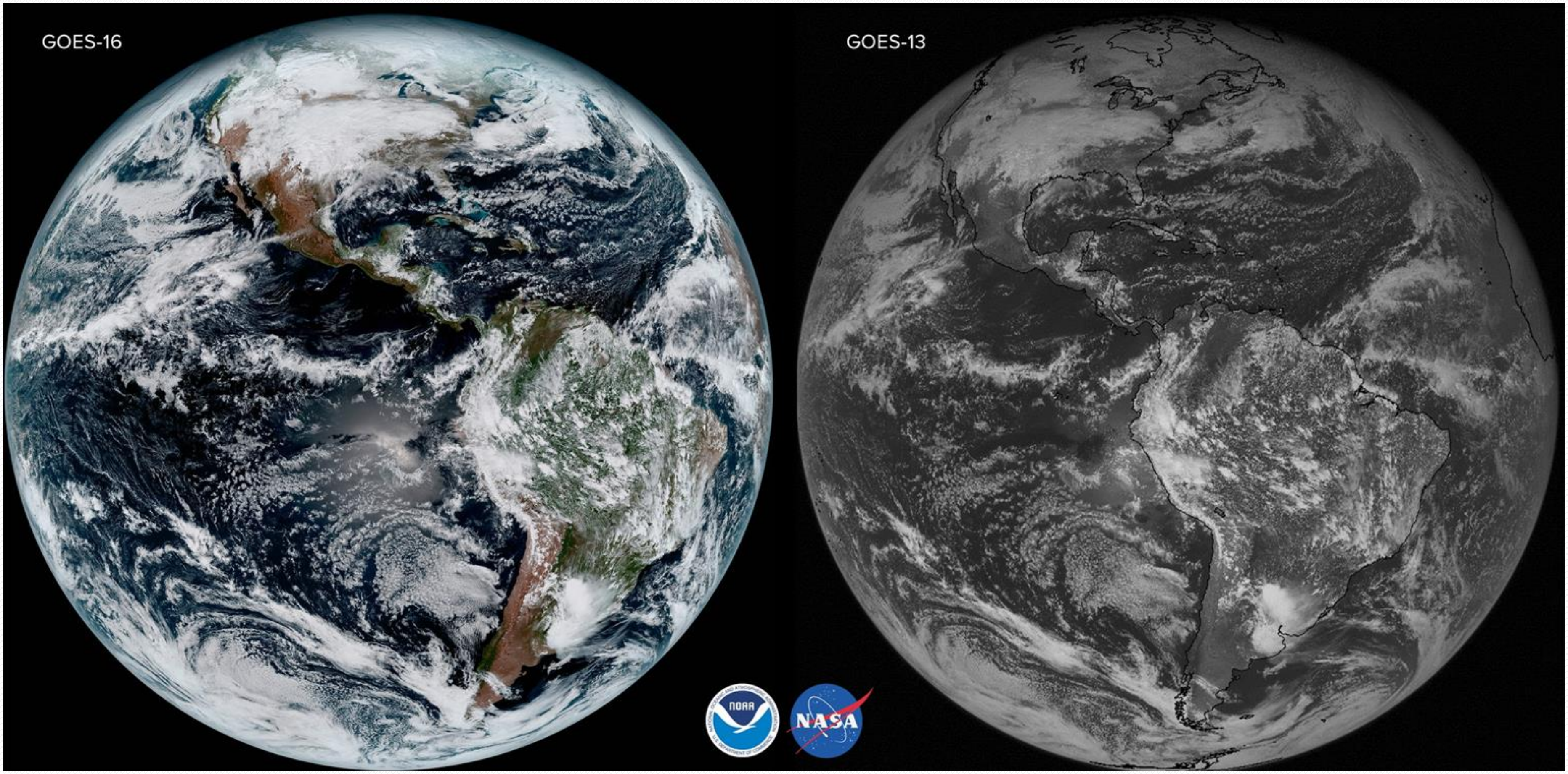
NOAA RESEARCH NOAA FISHERIES

Acknowledgements: *This program is a multi-institutional effort and we thank all the teams of contributors in supporting the design, development, and operations of these missions towards our common goals. We thank the officers and crew of the NOAA ship Oscar Dyson and Bell Shimada for their invaluable assistance during the Saildrone comparisons. This work is funded by NOAA-OAR and CPO.*

ITAE

GOES-R

GOES-16 vs GOES-13
JAN 2017



https://www.flickr.com/photos/noaasatellites/32441255306

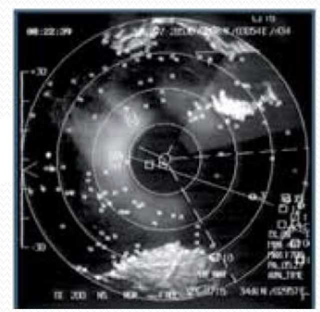
Challenges

WP-3D Lower Fuselage Radar Upgrade

Replace 360 degree scanning Lower Fuselage Weather Radar with AN/APY-11 Multimode Radar System

Inverse Synthetic Aperture (ISAR)

Weather, AIS, Air-to-Air

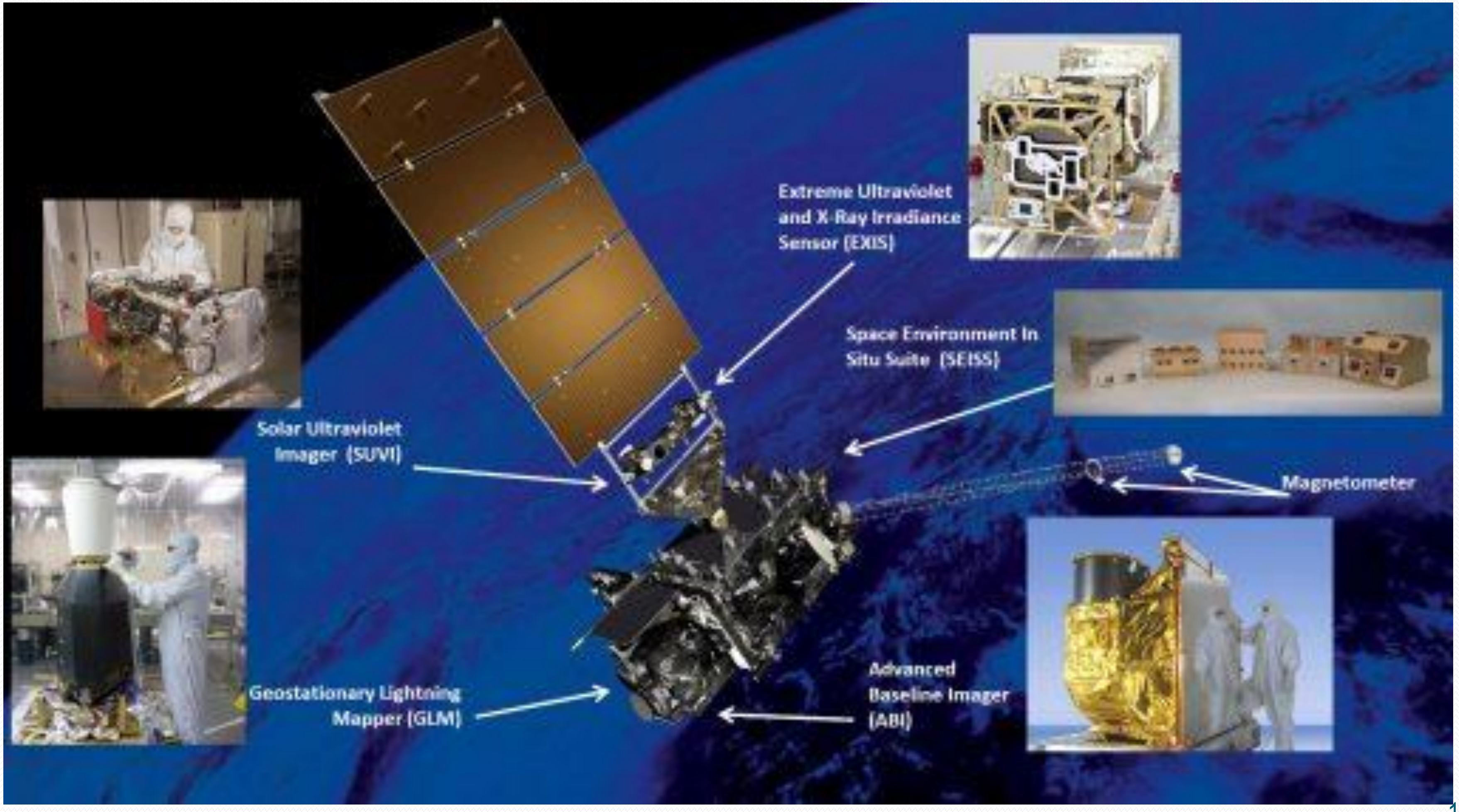


Synthetic Aperture (SAR)

16

GOES-16

Transition to operations and any remaining cal/val of the instruments and products, especially the Magnetometer



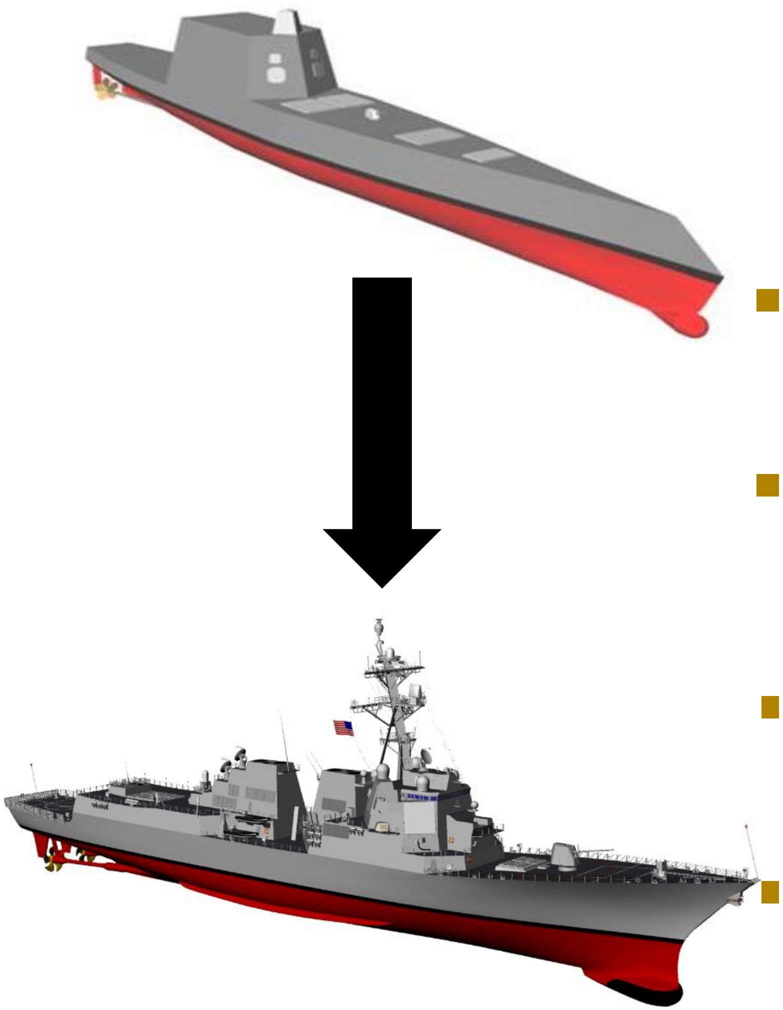
Thank You

Air and Missile Defense Radar (AMDR)

"Sea Power to the Hands of Our Sailors"

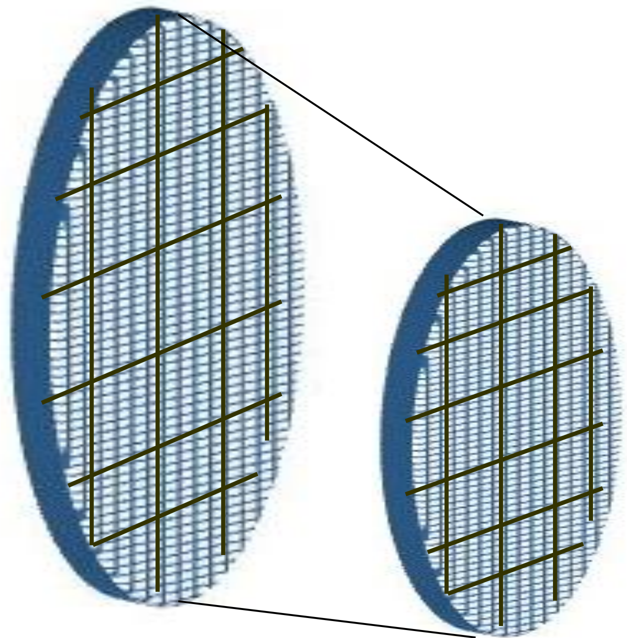
Presented by:
CAPT Seiko Okano
Major Program Manager (MPM)
PEO IWS 2.0 Above Water Sensors

AMDR Background



- Maritime Air and Missile Defense Joint Forces (MAMDJF) Analysis of Alternatives (AoA) results:
  - very large phased array radar (SPY +30dB) to be paired with a newly constructed combatant to meet the stressing BMD and cruise missile threats
- The Next-Generation Cruiser Program (CG(X)) was the planned combatant for AMDR,
- 2009 - a Radar/Hull Study was conducted
  - smaller AMDR could be paired with the DDG 51 hull and still meet these IAMD requirements
- USN canceled the CG(X) program, and restarted the DDG 51 shipbuilding program.
- New DDG 51 configuration with AMDR became known as DDG 51 Flight III

AMDR Challenges
Hardware Systems Engineering



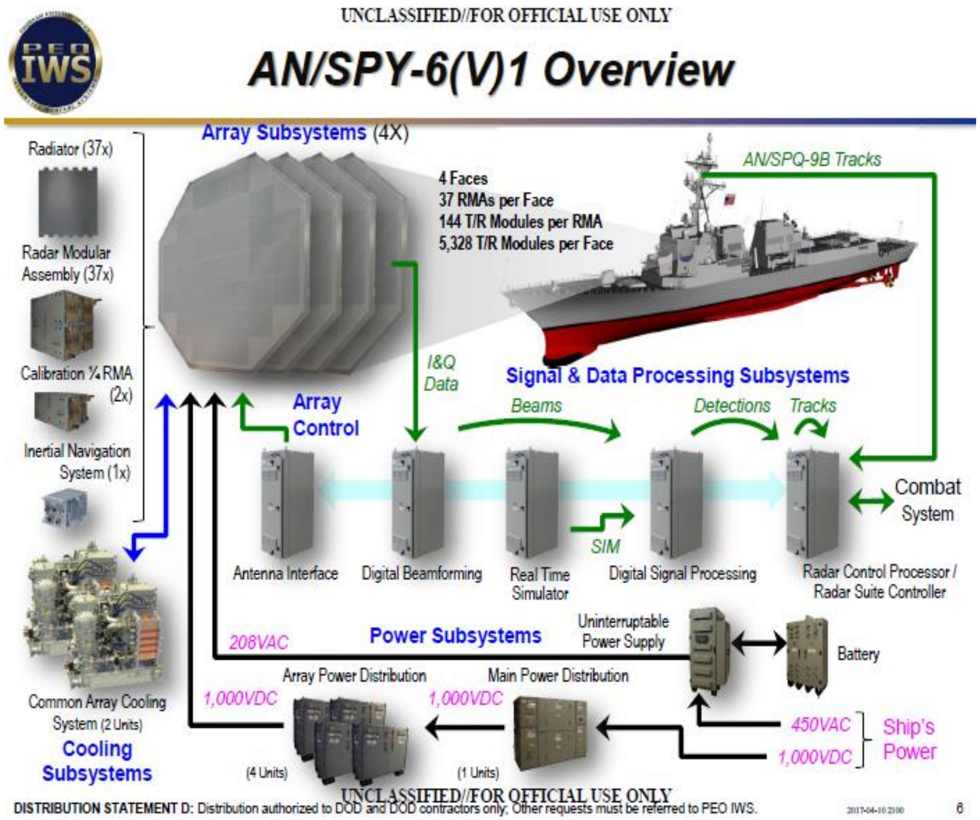
- **Scalability and Modularity**
  - IWS 2.0 partnered with ONR, OSD Title III/ManTech Offices, and Industry in an effort to make AMDR modular, scalable, affordable, and to reduce risk

- **Risk reduction Investments:**
  - **Gallium Nitride (GaN) Power Electronics**
    - OSD Title III
      - Conformal Hermetic Coating for Microelectronics
      - GaN on SiC MMIC Production for S and X-band Radar/EW Systems
    - Conducted follow-on ManTech GaN Producibility programs
  - **Digital Array Radar (DAR)**
    - ONR Future Naval Capability (FNC): Provided an active phased array radar that incudes the digital beamforming (DBF) architecture.
  - **Affordable Common Radar Architecture (ACRA)**
    - ONR FNC: Provided a modular and open combat system interface to integrate with the Product Line Architecture (PLA)
  - **Affordable Electronically Scanned Array Technology (AESAT)**
    - ONR FNC: Provided electronic components to reduce lifecycle costs in the next-generation active ESA radars
      - Components included: High Power/Efficiency MMICS and RF Power Amplifiers, Low Noise Digital Tx/Rx components, and DBF components

- **Open architecture (OA) standards, interfaces, and equipment were implemented into initial design for the radar front-end arrays, electronics and back-end processing**

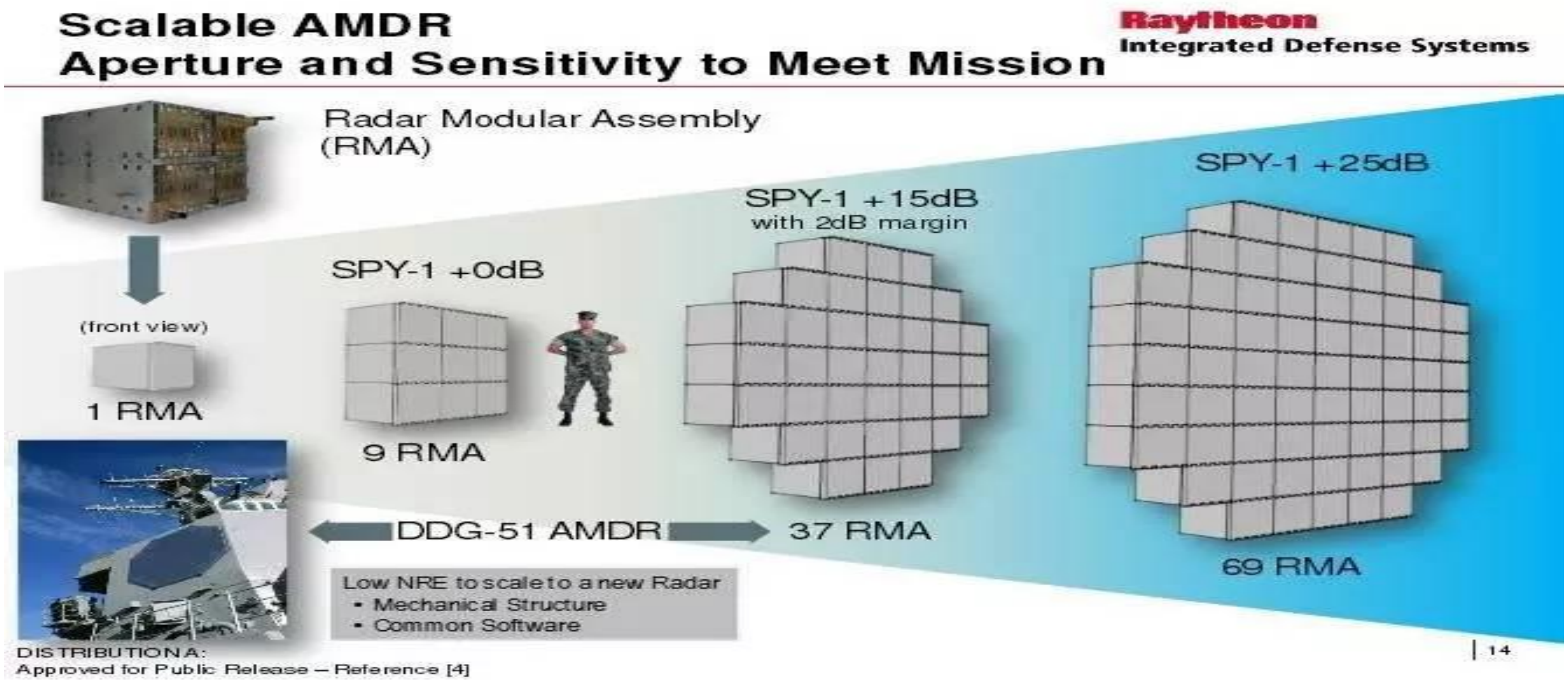
AMDR Hardware Systems Engineering

- **An active, digital radar enables multiple and simultaneous high-fidelity radar beams for a rapid volumetric search**
- **Implementation of the modular hardware and advancements in R&D achieved the following radar system and performance benefits:**
  - Eased the Systems Engineering Workload
    - Decreased the complexity of the radar design
  - Improved the integration and testing of the radar system
  - Active Performance
    - Improved detection sensitivity
    - Improved clutter attenuation
  - SS Reliability
    - Improved/Increased Mean Time Between Failure (MTBF)
      - 10^8 (100 Million) hours
    - Graceful Degradation Performance
  - Enables Digital Beamforming (DBF) Architecture
- **Cost Savings applied to the acquisition program**
  - Sustainment and Lifecycle costs also decrease



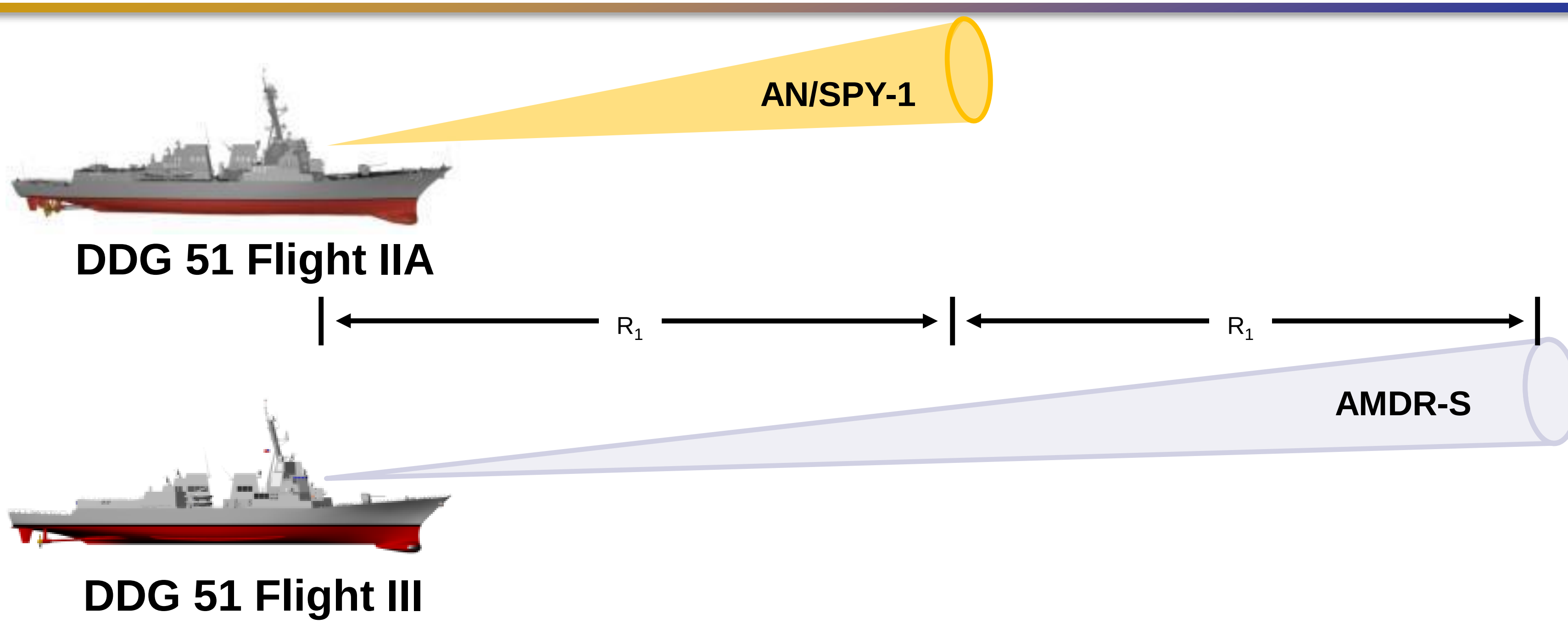
AMDR (AN/SPY-6) Hardware Overview

Final AMDR Array Design



- Each RMA measures 2’ x 2’ x 2’
  - Each RMA is essentially an individual radar
- This common architecture ensures the radar’s extensibility and scalability to other platforms, and their particular mission requirements
  - EASR is a derivative of AMDR that will be installed on CVNs and Amphibs
- Common and Open front/back-end architectures ensure:
  - Low NRE for future radar derivatives(radar scaling)
  - Common Logistics, Spares, Manning, and Training

AMDR Benefits



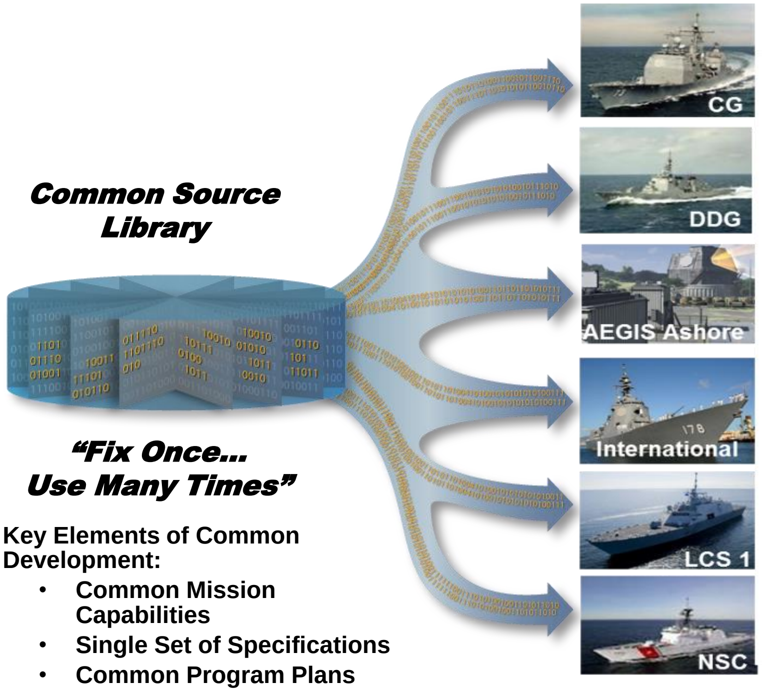
- AMDR-S will acquire and track a target *half the size* and at *twice the range* compared to the AN/SPY-1, providing increased flexibility in ship operating location
- Ability to react to and provide engagement data for the stressing Very Low Observable/Very Low Observable Flyer (VLO/VLOF) target in a dense clutter environment
- Capable of operating in natural and man-made environments to meet multi-mission requirements.

AMDR is in development to support robust IAMD (BMD and AAW) Raid Capability

AMDR Software Engineering

Radar-Combat Integration: Open SW Standards

- **Apply Product Line Architecture (PLA) principles to create common, open interfaces to enable integration**
  - Allows future radars the ability to integrate with other combat systems
  - Allows the USN to have 3rd party vendors develop and integrate additional capability into the radar and combat system.
- **Integration of SPY-6 into AEGIS**
  - Relied on a “modified” B/L 9 ACS and the AEGIS Common Source Library (CSL)
    - Developed new components and new interfaces
  - Demonstrated successful simulation of the AAW and BMD Fire Control Loops
  - Significant ROI for B/L 10 (ACB-20) for future integration and testing
  - Significant reduction of NRE for integration/testing into other combat systems (e.g. SSDS)



Key Elements of Common Development:

- **Common Mission Capabilities**
- **Single Set of Specifications**
- **Common Program Plans**
- **Single Set of Processes & Metrics**
- **Integrated Team Structure**
- **Enterprise Products**

QUESTIONS?

"Sea Power to the Hands of Our Sailors"

DISTRIBUTION STATEMENT D: Distribution authorized to DOD and DOD contractors only; Other requests must be referred to PEO IWS.

Backups

Executive Panel: Interagency Systems Engineering

Moderator:

Ms. Kristen Baldwin

Deputy Assistant Secretary of Defense for Systems Engineering (Acting)

Panel Members:

- **Mr. Jon Holladay**
  - Technical Fellow for Systems Engineering
    National Aeronautics and Space Administration (NASA)
- **Mr. Kent Jones**
  - Assistant Deputy Administrator for Systems Engineering and Integration
    Defense Programs, National Nuclear Security Administration (NNSA)
- **Mr. Joseph Post**
  - Deputy Director, Systems Engineering and Integration
    U.S. Federal Aviation Administration (FAA)
- **Mr. Albert "Benjie" Spencer**
  - Chief Engineer and Director of Engineering Standards Division
    National Oceanic and Atmospheric Administration (NOAA)
- **Mr. James Tuttle**
  - Chief Systems Engineer, Science and Technology Directorate
    Department of Homeland Security (DHS)

NDIA 20th Annual Systems Engineering Conference

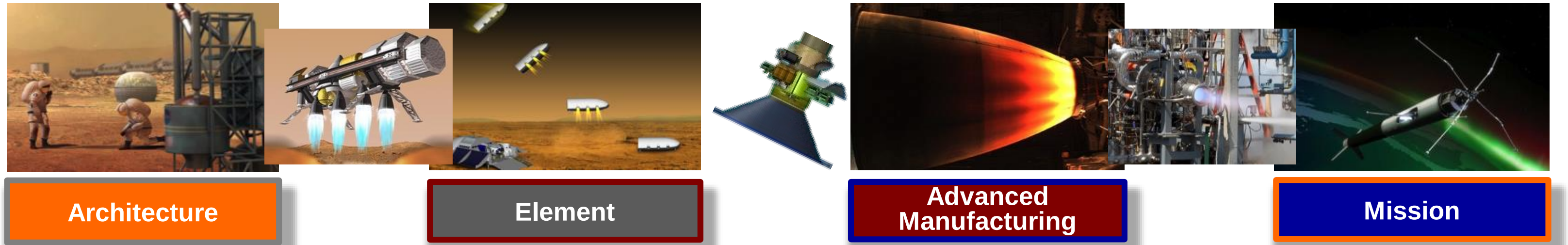
Panel Discussion:
NASA Systems Engineering

Jon B. Holladay
NASA Technical Fellow, Systems Engineering
October 24, 2017

Key 2017 Systems Engineering Accomplishments

- Engaged Systems Engineering Capability Leadership Team toward:
  - ***Understanding*** of state of discipline via deep dive assessment
  - ***Aligning*** capability needs across Centers and Missions
  - ***Optimizing*** capability vector focused thru both tactical and strategic domains

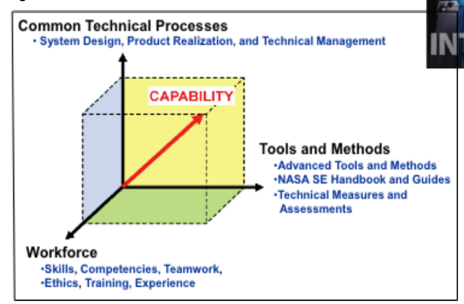
- Completed Model-Based System Engineering (MBSE) Pathfinder Part 2:
  - ***Increase*** stakeholder involvement, horizontally and vertically
  - ***Demonstrate*** applications across product life-cycle
  - ***Engage*** the future state of NASA Systems Engineering



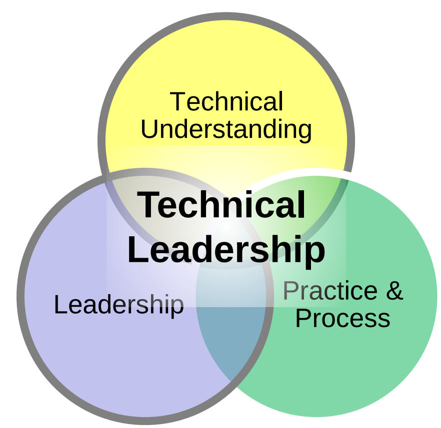
Systems Engineering Area of Emphasis for 2018

- Expand utilization of the new digital NASA SE Handbook
  https://www.nasa.gov/connect/ebooks/nasa-systems-engineering-handbook

- Complete NASA SE Policy (NPR 7123.1B) revision



- Continue refinement of Agency's SE Strategic vector
  - Focus on Technical Leadership
  - Recognize the complexity and dynamic quality of environment
  - Recognize the need to interface and partner beyond NASA



NDIA SE Conference
Program Manager Panel Questions

Panel Theme:
DoD Executive Panel: Service and Agency Program Managers discussion:

"Teaming with systems engineering to shape and control risk, manage issues, and seize upon opportunities to deliver superior warfighting capabilities."

Moderator: Col. David McIllece, USAF

Panelists:
1. CAPT Seiko Okano, PEO Integrated Warfare Systems (IWS)
2. COL Mike Milner, Armored Multi-Purpose Vehicle (AMPV) PM
3. Col Edward Hospodar, GPS User Equipment SML
4. Col Amanda Myers, Deputy Director, Global Reach Programs; former C-17 SPM

General Systems Engineering

#	Question	Okano	Milner	Hospodar	Myers
1	What are you most proud of in your program's SE activities? What is your program doing that others might not be doing to make your systems engineering program successful?			X Security Engineering	
2	Please tell a SE Success/horror stories/lessons learned.				
3	What do you value from your systems engineers now, what you would like to get, what would you prefer less of (topics/communication, etc)?				
4	Please discuss your program's Risk Management approach, and its value. What is the role/participation of the prime contractor?				
5	What would you say is the most important issue or problem for systems engineers to understand about program management?				
6	Has your view/use of systems engineering changed over the years and across programs you have worked? Are there different approaches for different programs vs. one size fits all?				
7	What observations/lessons to you have regarding the systems engineering roles of the program office, prime contractors and other stake holders (e.g., technical authorities)? What are the strengths/weaknesses of how the roles are distributed and executed?			X Importance of early SE and trade studies during requirements definition	
8	Most of SE life cycle emphasis is on the program development during the early phases. Is there value and how can SE be extended to address the entire lifecycle?				

Organic Engineering / Risk Management

#	Question	Okano	Milner	Hospodar	Myers
1	Topic: Strengthening organic engineering and other technical capabilities in our own workforce: **Question**: **In your programs, where do you see the greatest need for strengthening engineering capabilities? (Quantity, quality, specialized skill sets, etc.)**			X Quality analysis and verification vs. SE process focus	
2	Topic: Understand and mitigate <u>technical</u> risk. **Questions:** - **How do you differentiate "programmatic" risks such as a funding risk, from "<u>technical</u> risks" such as not meeting requirements or software development risks?** - **Do you have more control over mitigation activities for technical risks than you do with programmatic risks?** - **Do you have constraints in identifying technical risks in your programs? If so, please discuss.**			X Stakeholder engagement presents opportunities to "revisit" requirements which is a programmatic risk but can yield insight into use cases and lowers risk to OT&E	
3	Topic: Advantages for programs with rigorous risk management practices. **Questions:** - **What can we do to encourage programs managers to enact sound risk management processes?** - **What common barriers stand in the way of enacting these processes?** - **What experiences can you share that will help programs to smartly accept/manage increased risk in order to achieve greater and/or faster successful outcomes?**			X Importance of prototyping and early integration into the architecture and next level of assembly for feedback or to determine missing requirements	
4	Topic: The Department recently issued an updated guide for Risk Management: The DoD Risk, Issue, and Opportunity (aka "RIO") Management Guide for Defense Acquisition Programs. **Questions:** - **How have you applied RIO concepts (such as Issue Management, Opportunity Management, Cross-Program Risk Management, etc.) in your overall risk mitigation approach?** - **Do you have any best-practices or other experiences that can inform/improve the RIO approach?**				

Panelist-Suggested Questions

#	Question	Okano	Milner	Hospodar	Myers
1	Please feel free to offer any questions you would like included… **Question: <<text here>>**				

Executive Panel: DoD Systems Engineering

Panel Members:

- **Ms. Kristen Baldwin**
  - Acting Deputy Assistant Secretary of Defense for Systems Engineering
- **Mr. Leo Smith, USA**
  - Division Chief, Systems Engineering Program Support
    ASA(ALT) System of Systems Engineering and Integration
- **Mr. William Bray, USN**
  - Deputy Assistant Secretary of the Navy for Research, Development, Test and Evaluation
- **Col Laird Abbott, USAF**
  - Chief, Engineering and Force Management Division, Deputy Assistant Secretary of the Air Force for Science, Technology and Engineering

DoD Systems Engineering Opportunities

Ms. Kristen Baldwin

Acting Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))

20th Annual NDIA Systems Engineering Conference

Springfield, VA | October 24, 2017

Defense Research & Engineering Strategy

Mitigate current and anticipated threat capabilities

Enable new or extended capabilities affordably in existing military systems

Create technology surprise through science and engineering

Focus on Technical Excellence

Deliver Technologically Superior Capabilities

Grow and Sustain our S&T and Engineering Capability

DoD Engineering Focus Areas

- Grow and maintain engineering and technical leadership talent
- Mature engineering practices to implement modularity, agility, and innovation into systems
- Leverage advanced analytical and computing technologies and migrate to digital acquisition, engineering and manufacturing practice
- Address complex software development, integration, and sustainment challenges
- Establish practices for cyber-resilient aerospace and defense systems
- Enable trust and access to assured hardware and software
- Implement enterprise and mission integration management capabilities

US Air Force Engineering Enterprise

An Update to the NDIA SE Conference

Col Laird Abbott
SAF/AQR

Air Force Engineering Enterprise
Cross Cutting Strategic Direction

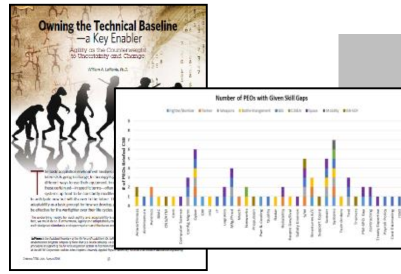
Key Leadership Focus Areas

Own Technical Baseline

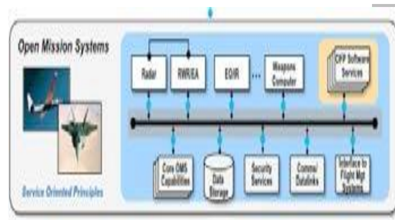
Open Systems

Modeling & Simulation

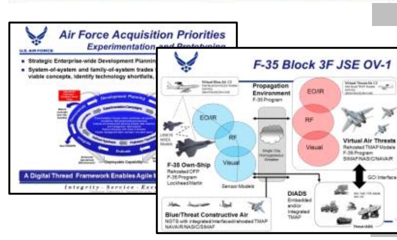
Cyber



- Regain Gov't Control of Pgms
- Informed Decision Making
- Skill-gap Identify/Mitigate



- Industry Consensus Tech Solutions
- Open Key-Interfaces
- Service Oriented Architectures
- Common Messaging Language



- Joint Simulation Environment
- Inventory M&S + Develop Regmts
- Enable Experimentation/Prototyping

- Cyber Campaign Plan
- Cyber Workforce
- Risk Id & Management
- Process & Policy Dev

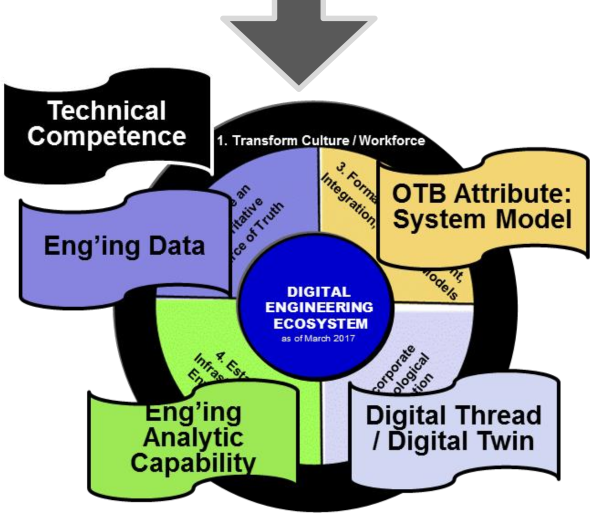
The AF EE Challenge Problem

Digital Engineering

- **Given complexity, uncertainty and the lack of agility have diminished Air Force Acquisition’s ability to meet mission needs**
- **How do we establish an all digital authoritative source of life cycle technical data for every weapon system**
- **In order to deliver more capability more rapidly then ever before**

OWNING THE TECHNICAL BASELINE

- Technical Competence
- Engineering Data
- Engineering Analytic Capability



Digital Engineering ≈
Owning the Technical Baseline <u>DIGITALLY</u>

The End

Executive Panel: Interagency Systems Engineering

20th NDIA SE Conference, Waterford, Springfield, VA
Tuesday, October 24, 2017
11:15 - 12:30 am

Questions

1. It's been roughly 10 years since INCOSE kicked off their MBSE initiative. The IAWG just released a white paper this year that talked challenges of MBSE infusion. What are your thoughts on where are in the adoption process and how long will it take until it's an everyday thing.

2. If you could only pick one thing as the focus to improve the efficiency of your System Engineering response, what would it be and why?

3. What's the hardest thing about your job…

Program Managers Panel

Moderator: **Col David McIllece, USAF**

Deputy for Systems Engineering Plans and Policy, ODASD(SE)

***Panel Members*:**

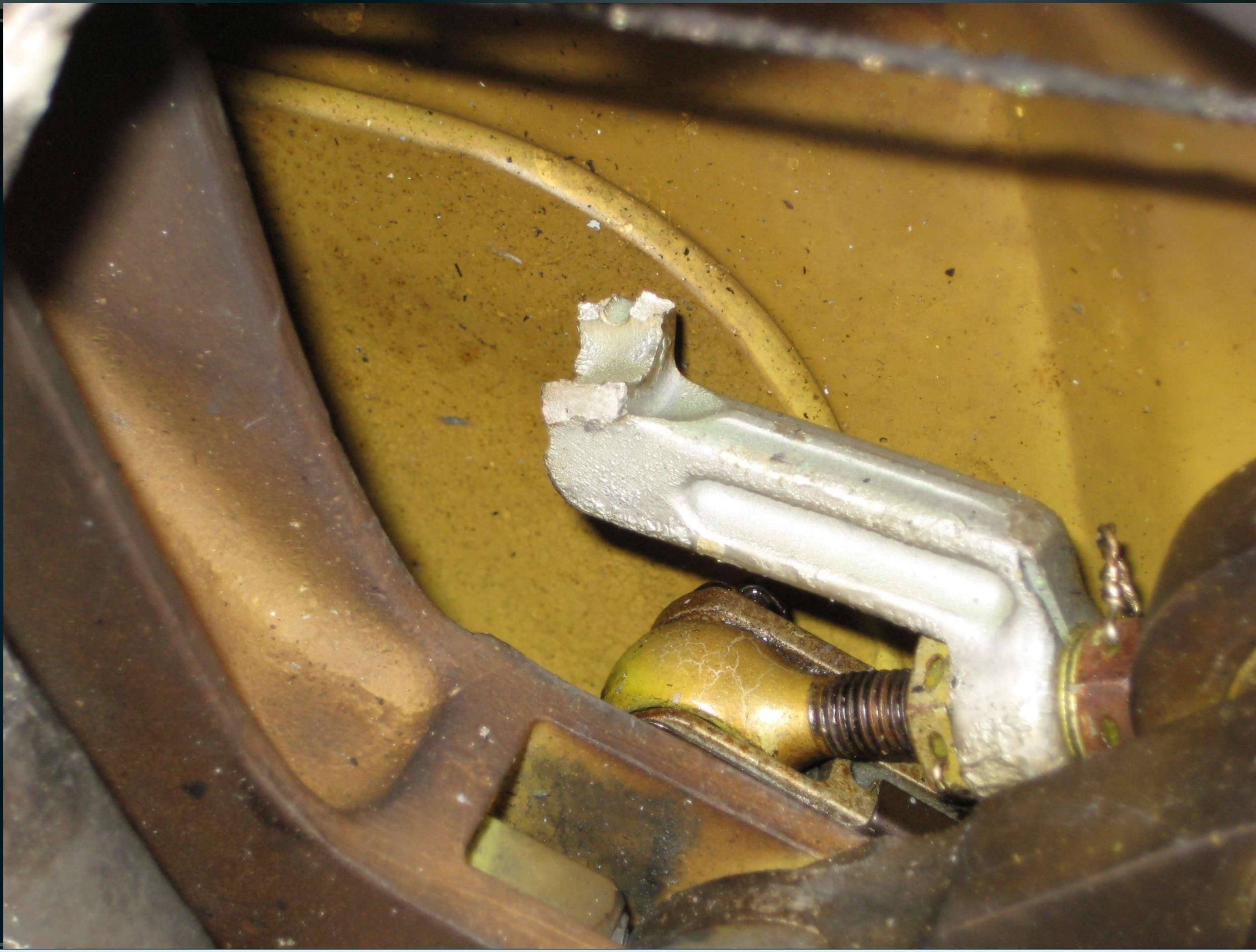
- **COL Michael Milner, USA**
  - Project Manager, Armored Multi-Purpose Vehicle (AMPV)
- **Col Amanda Myers, USAF**
  - Deputy Director, Global Reach Programs
  - Former C-17 System Program Manager
- **CAPT Seiko Okano, USN**
  - Major Program Manager, PEO Integrated Warfare Systems (IWS) 2.0
- **Col Edward Hospodar, USAF**
  - Senior Materiel Leader, GPS User Equipment Division, Space and Missile Systems Center

Col Amanda Myers
Deputy Director, Global Reach Programs
SAF/AQQ


RA
AF
66 389
U.S. AIR FORCE
RA


U.S. AIR FORCE
0066

Safe
Suitable
Effective



Sustaining Engineering

- C-17 Strategic Goal: Increase focus on OSS&E & "Own the Technical Baseline"
  - Grow Organic Sustaining Engineering skills
  - Relook at engineering processes; ensure proper alignment between USG and OEM
  - Robust integrity programs
  - Proactively identify watch areas
  - Increasing USG oversight/rigor
- Transition from production driven focus to: aircraft aging, corrosion, DMS/Obsolescence


U.S. AIR FORCE
3121

Space and Missile Systems Center

Military GPS User Equipment Modernization

NDIA

20th Annual Systems Engineering Conference

Col Ed Hospodar
Chief, GPS User Equipment Division
Global Positioning Systems Directorate

1966 Aerospace Corporation "Navigation Satellite Study"

SPACE AND MISSILE SYSTEMS CENTER

[redacted]

UNCLASSIFIED

REPORT NO.
TOR-1001(2525-17)-1

(U) Briefing– Navigation Satellite Study

24 AUGUST 1966

Prepared by J. B. WOODFORD and H. NAKAMURA
System Planning Division

Prepared for COMMANDER SPACE SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
LOS ANGELES AIR FORCE STATION
Los Angeles, California

CLASSIFICATION CHANGED TO [redacted] Unclassified
By Authority of ADG/4
By AOC 1B Date 10/16/79
[redacted]

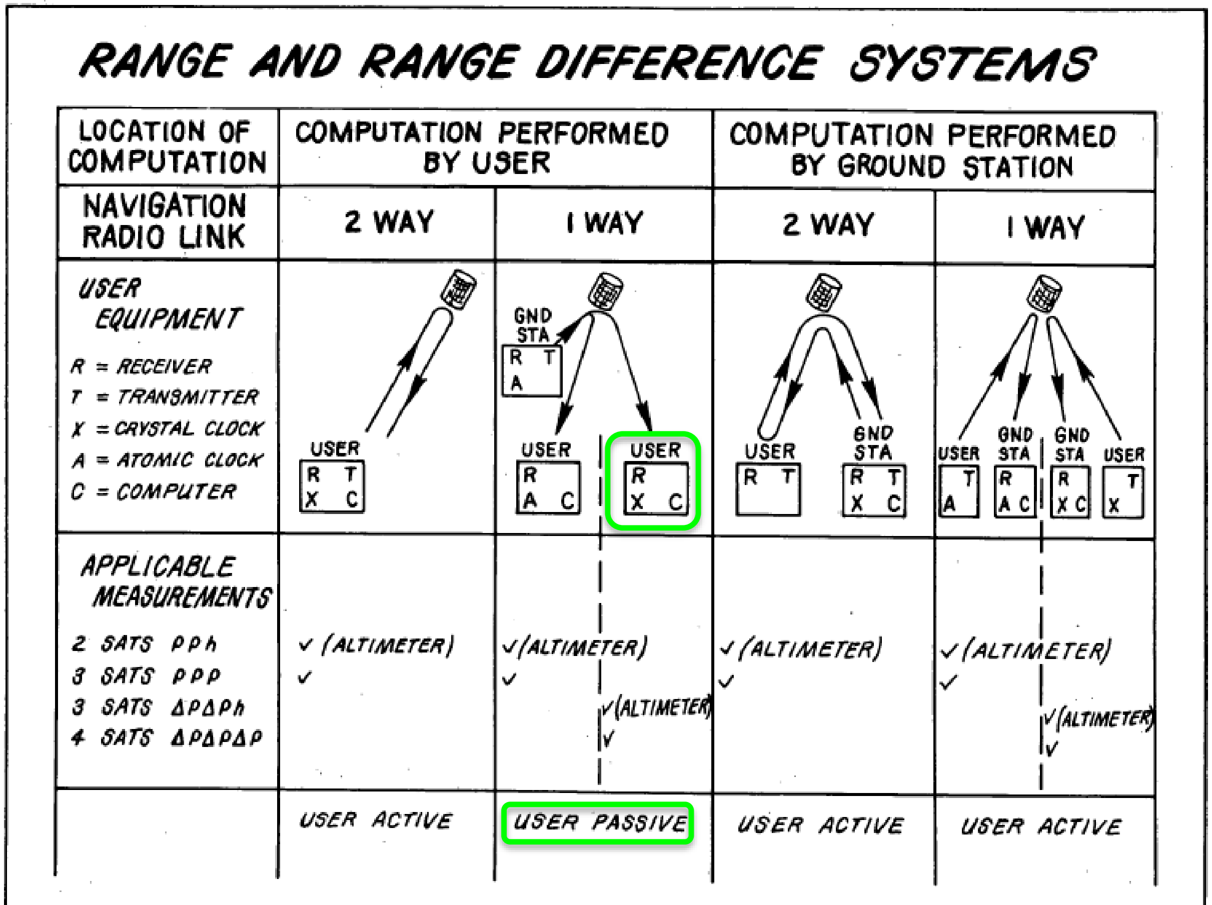
EL SEGUNDO TECHNICAL OPERATIONS • AEROSPACE CORPORATION
CONTRACT NO. AF 04(695)-1001

UNCLASSIFIED

[redacted]

1966 Aerospace Corporation “Navigation Satellite Study”

SPACE AND MISSILE SYSTEMS CENTER



RANGE AND RANGE DIFFERENCE SYSTEMS

LOCATION OF COMPUTATION	COMPUTATION PERFORMED BY USER		COMPUTATION PERFORMED BY GROUND STATION	
NAVIGATION RADIO LINK	2 WAY	I WAY	2 WAY	I WAY
USER EQUIPMENT R = RECEIVER T = TRANSMITTER X = CRYSTAL CLOCK A = ATOMIC CLOCK C = COMPUTER	USER R T X C	GND STA R T A USER R A C USER R X C	USER R T GND STA R T X C	USER T A GND STA R A C GND STA R X C USER T X
APPLICABLE MEASUREMENTS 2 SATS ρρh 3 SATS ρρρ 3 SATS ΔρΔρh 4 SATS ΔρΔρΔρ	✓ (ALTIMETER) ✓	✓(ALTIMETER) ✓ ✓(ALTIMETER) ✓	✓ (ALTIMETER) ✓	✓(ALTIMETER) ✓ ✓(ALTIMETER) ✓
	USER ACTIVE	USER PASSIVE	USER ACTIVE	USER ACTIVE

- 1-way ranges, passive receivers, crystal oscillators
- Passive (one-way) reduces UE power and avoids detection
- Internal computer spreads the burden for 1,000’s of users and avoids sending measurements
- Crystal oscillator minimizes UE SWAP-C and doesn’t hurt accuracy
- Autonomous receivers

SWAP-C = Size, Weight, and Power - Cost

The widespread use of GPS and duplication by all other GNSS validate these choices

GPS Overview

Civil Cooperation
- 3+ Billion civil & commercial users worldwide
- Search and Rescue
- Civil Signals
  - L1 C/A (Original Signal)
  - L2C (2nd Civil Signal)
  - L5 (Aviation Safety of Life)
  - L1C (International)

Department of Defense
- Services (Army, Navy, AF, USMC)
- Agencies (NGA & DISA)
- US Naval Observatory
- PNT EXCOM
- GPS Partnership Council

Spectrum
- World Radio Conference
- International Telecommunication Union
- Bilateral Agreements
- Adjacent Band Interference

35 Satellites / 31 Set Healthy
Baseline Constellation: 24 Satellites

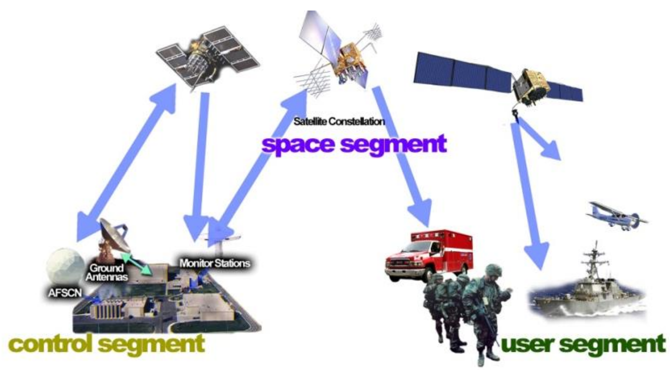
Satellite Block	Quantity	Average Age	Oldest
GPS IIR	12	15.7	20.1
GPS IIR-M	7	10.1	11.9
GPS IIF	12	3.6	7.3
Constellation	31	9.7	20.1

AS OF 1 SEP 17

Maintenance/Security
- All Level I and Level II
  - Worldwide Infrastructure
  - NATO Repair Facility
- Develop & Publish ICDs Annually
  - Public ICWG: Worldwide Involvement
  - Materials Available at: gps.gov/technical/icwg
- Update GPS.gov Webpage
- Load Operational Software on over 970,000 SAASM Receivers
- Distribute PRNs for the World
  - 120 for US and 90 for GNSS

Department of Transportation
- Federal Aviation Administration

Department of Homeland Security
- U.S. Coast Guard

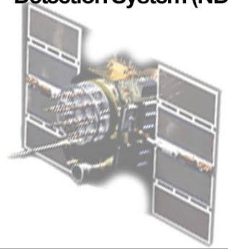


International Cooperation
- 57 Authorized Allied Users
  - 25+ Years of Cooperation
- GNSS
  - Europe - Galileo
  - China - Beidou
  - Russia - GLONASS
  - Japan - QZSS
  - India - NAVIC

GPS Modernization

Space System (Satellites)

Legacy (GPS IIA/IIR)
- Basic GPS
- NUDET (Nuclear Detonation) Detection System (NDS)



GPS IIR-M
- 2nd Civil signal (L2C)
- New Military signal
- Increased Anti-Jam power

GPS IIF
- 3rd Civil Signal (L5)
- Longer Life
- Better Clocks

GPS III (SV01-10)
- Accuracy & Power
- Increased Anti-Jam power
- Inherent Signal Integrity
- Common L1C Signal
- Longer Life

GPS III (SV11+)
- Unified S-Band Telemetry, Tracking & Commanding
- Search & Rescue (SAR) Payload
- Laser Retroreflector Array
- Redesigned NDS Payload
- Regional Military Protect (RMP)

Ground System

Legacy (OCS)
- Mainframe System
- Command & Control
- Signal Monitoring

AEP
- Distributed Architecture
- Increased Signal Monitoring Coverage
- Security
- Accuracy
- Launch And Disposal Operations

OCX Block 0
- GPS III Launch & Checkout

GPS III Contingency Ops (COps)
- GPS III Mission on AEP

M-Code Early Use (MCEU)
- Operational M-Code on AEP

OCX Block 1
- Fly Constellation & GPS III
- Begin New Signal Control
- Upgraded Information Assurance

OCX Block 2+
- Control all signals
- Capability On-Ramps
- GPS III Evolution

User Equipment System (Receivers)

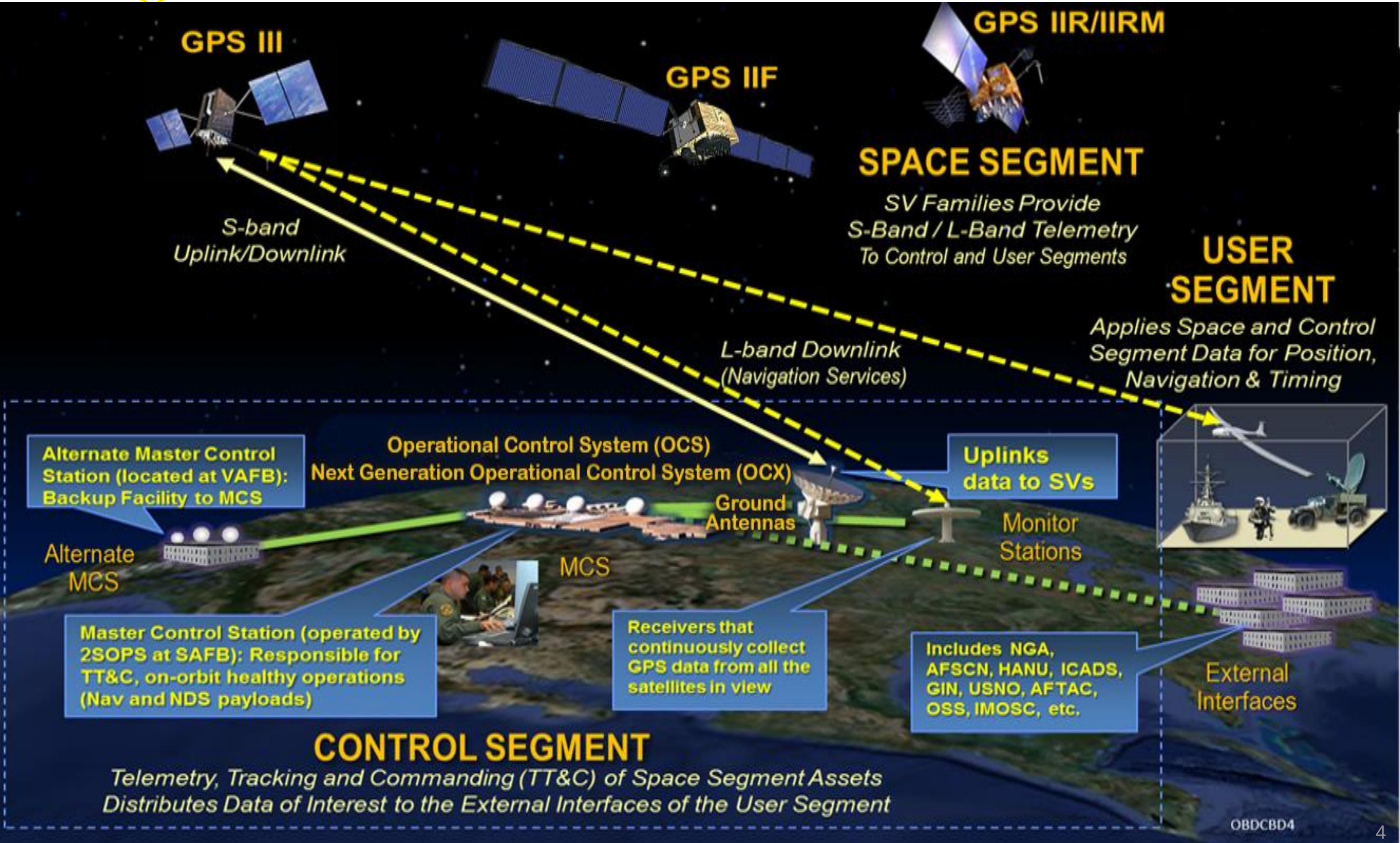
Legacy (PLGR/GAS-1/MAGR)
- First Generation System

User Equipment
- Improved Anti-Jam & Systems
- Reduced Size, Weight & Power

Upgraded Antennas
- Improved Anti-Jam Antennas

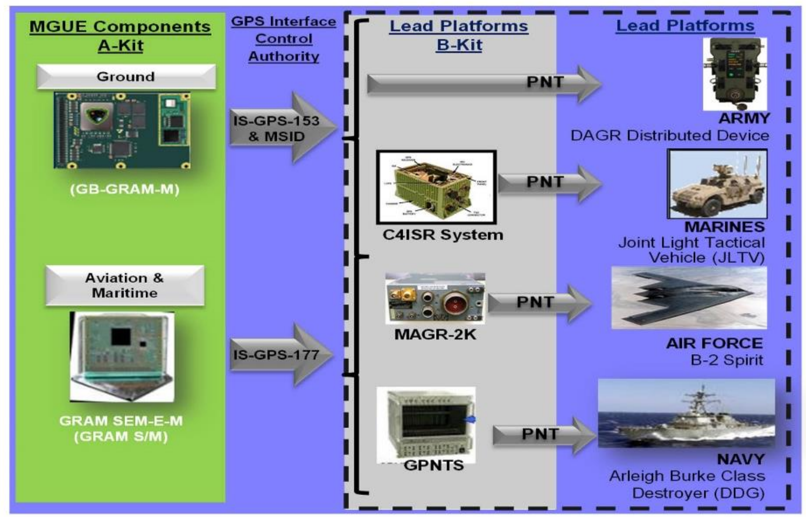
Modernized
- M-Code Receivers
- Common GPS Modules
- Increased Access/ Power with M-Code
- Increased Accuracy
- Increased Availability
- Increased Anti-Tamper/ Anti- Spoof
- Increased Acquisition in Jamming

GPS Enterprise Operational View



Military GPS User Equipment (MGUE)

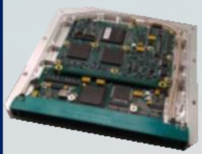
- Commercial market-driven acquisition approach
- Three vendors developing modernized receiver cards
  - Ground form factor
  - Aviation/Maritime form factor
- Current Status
  - L-3 Technologies first to receive security certification Oct 2016
  - Developmental testing ongoing
  - Conducting early integration activities to support Service-nominated Lead Platforms



Military GPS User Equipment

Prototype GPS Receiver Flight Tested on B-2

SPACE AND MISSILE SYSTEMS CENTER



Prototype Military GPS User Equipment Receiver Card

Prototype Miniaturized Airborne GPS Receiver

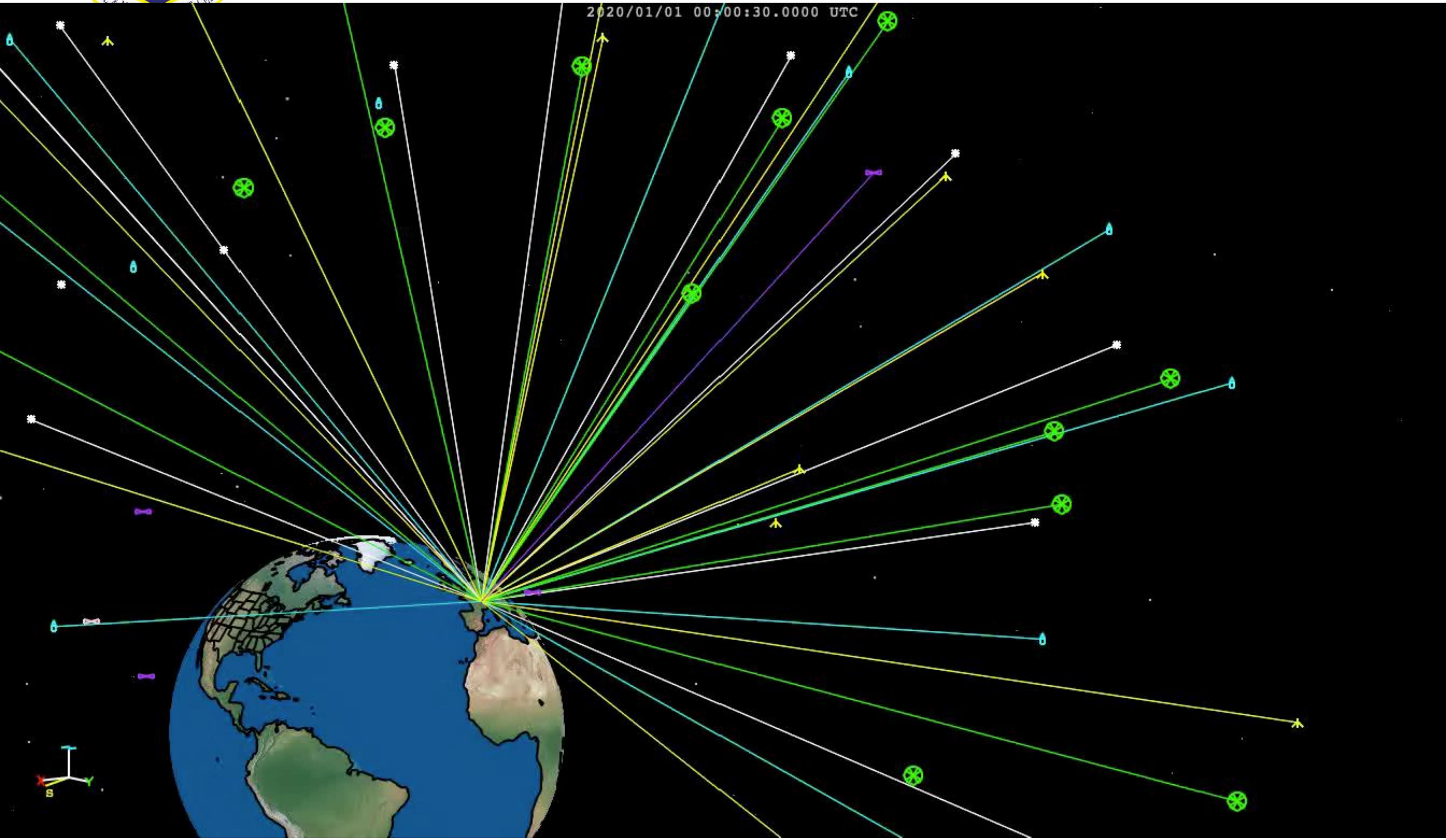
4 Successful B-2 Test Flights

Military GPS User Equipment Demonstrated in B-2

UNCLASSIFIED//APPROVED FOR PUBLIC RELEASE

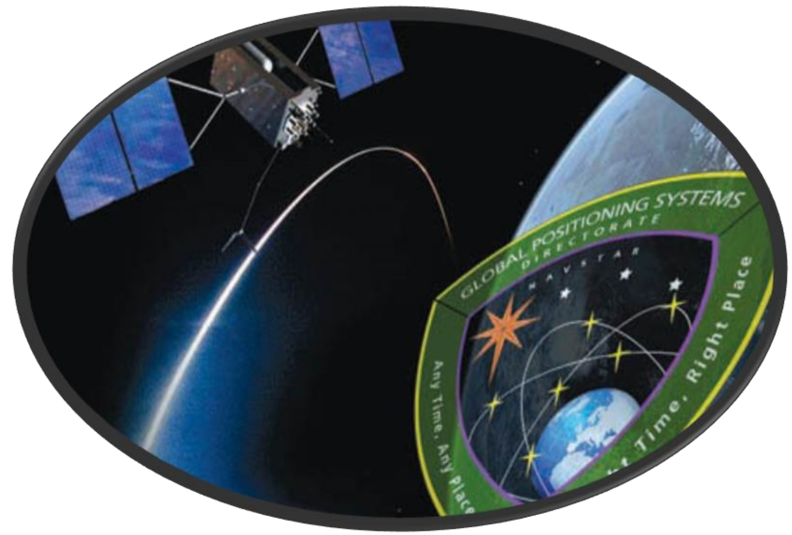
MGUE Precision Guided Munitions Test

Looking Ahead: Multi-GNSS



Perspectives

- GPS is <u>the</u> Global Utility
  - Committed to maintaining uninterrupted service
  - “The Gold Standard”
- Modernizing to enhance GPS resiliency by:
  - Upgrading all three segments
  - Moving to M-Code
  - Adding civil signals
- Exploring multi-GNSS potential



Deliver capabilities, execute with excellence, lead with transparency